EEE

IALOG(R)File 351:DERWENT WPI
c)1995 Derwent Info Ltd. All rts. reserv.

09873196 WPI Acc No: 94-153109/19
RPX Acc No: N94-120267
Electronic system implementing game of chance - uses portable electronic unit to play game of chance and encrypts data on win for validation by payment station.
atent Assignee: (INFO-) INFO TELECOM SA; (FRJE-) LA FRANCAISE JEUX; (REIB/) REIBEL J
uthor (Inventor): BIGONNEAU E; BOUEDEC J; REIBEL J; SIMON P
mber of Patents: 005
mber of Countries: 020
atent Family:

CC Number	Kind	Date	Week	
EP 596760	A1	940511	9419	(Basic)
FR 2697653	A1	940506	9421	
AU 9347459	A	940519	9424	
BR 9303955	A	940524	9424	
CA 2107249	A	940505	9429	

iority Data (CC No Date): FR 9213239 (921104)
plications (CC,No,Date): CA 2107249 (930929); EP 93402359 (930927); AU 9347459 (930921); BR 933955 (930929)
nguage: French
and/or WO Cited Patents: EP 450520; WO 8902139; WO 9106931
signated States
Regional): AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT ; SE
stract (Basic): EP 596760 A

The electronic unit is housed in a portable enclosure (11). It has circuits to store a set of reference data, and to compare this data with game data introduced by the player through a communication interface. One of the two data sets is a randomly generated value.

The gain from a successful result is stored in a memory. This is encrypted and stored. An input/output interface (17) allows the portable unit to communicate with an external station (11) which responds to requests for payment by the player. The encrypted data from the portable unit is decrypted, and compared with the request from the player. If the two agree payment is made from the station.

ADVANTAGE Allows player to engage in game of chance at any time they choose.

Dwg.1/10

e Segment: EPI
went Class: T05;
Pat Class: A63F-003/06; A63F-009/24; G06F-015/21; G06F-015/44; G07C-015/00; G07F-017/32
ual Codes (EPI/S-X): T05-F; T05-H05E; T05-H08C

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 697 653**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **92 13239**

(51) Int Cl⁵ : G 07 C 15/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 04.11.92.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 06.05.94 Bulletin 94/18.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *Société anonyme dite: INFO TELECOM* — FR et *Société anonyme d'économie mixte dite: LA FRANCAISE DES JEUX* — FR.

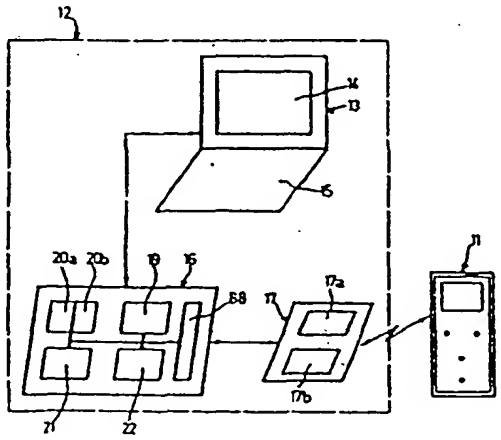
(72) Inventeur(s) : Reibel Jean-Michel, Simon Pierre-Luc, Digonneau Eric et Bouedec Jean-Etienne.

(73) Titulaire(s) :

(74) Mandataire : Bureau D.A. Casalonga - Josse.

(54) Dispositif électronique de jeu de hasard.

(57) Un boîtier portable (11) comprend des moyens de mémoire aptes à stocker au moins une donnée de référence, et des moyens de comparaison aptes à comparer ladite donnée de référence avec une donnée de jeu introduite par le joueur par une interface de communication, l'une de ces deux données étant une valeur générée de façon aléatoire. Une information de gain dépendant au moins du résultat de ladite comparaison, est stockée dans les moyens de mémoire, et des moyens de cryptage-boîtier sont aptes, en réponse à une information prédéterminée de demande de paiement (IDP) reçue, à établir une première valeur de gain cryptée à partir de ladite information de gain. Une station (12), externe au boîtier (11), comprend une interface-système d'entrée/sortie (17) apte à coopérer avec l'interface du boîtier, et des moyens de traitement-système (18), aptes, en présence d'une demande de paiement émanant du joueur, à lire ladite information de gain contenue dans les moyens de mémoire du boîtier. Des moyens de cryptage-système (19), homologues des moyens de cryptage-boîtier, établissent une deuxième valeur de gain cryptée à partir de ladite information de gain lue. Le paiement effectif du gain au joueur est conditionné par la concordance des deux valeurs de gain cryptées.



FR 2 697 653 - A1

Dispositif électronique de jeu de hasard.

L'invention concerne un dispositif électronique de jeu de hasard.

On connaît actuellement différents jeux de hasard permettant à un joueur de gagner des sommes d'argent moyennant le paiement d'une mise de départ. Ainsi, par exemple dans le jeu appelé "loto" (marque déposée) le joueur coche une série de chiffres sur un ticket qu'il fait valider auprès d'un organisme spécialisé en en acquittant un prix correspondant à la mise de départ. Un tirage au sort ultérieur est effectué sous contrôle dans un endroit choisi et, les joueurs en possession d'un ticket gagnant peuvent retirer leur gain auprès d'un organisme payeur.

Par rapport à ces jeux classiques, nécessitant un support papier et des tirages au sort à des dates prédéterminées et valables pour tous les joueurs, l'invention propose un concept radicalement différent de dispositif de jeu de hasard.

Un but de l'invention est de proposer un boîtier autonome et portable destiné à permettre à un joueur d'effectuer une ou plusieurs épreuves de jeu de hasard, la réussite ou l'échec auxdites épreuves conditionnant un score ou un niveau de gain suivant des règles de jeu prédéterminées. Ce boîtier constitue alors également l'élément de transaction pour le paiement du gain et comporte tous les éléments nécessaires à la vérification de ce gain. Outre ce boîtier portable et autonome, il est prévu un système de contrôle, externe au boîtier, permettant à l'organisme payeur d'effectuer les vérifications nécessaires avant le paiement du gain.

L'invention a encore pour but de permettre d'effectuer au sein même du boîtier électronique, le tirage au sort des données de référence par rapport auxquelles seront comparées les données de jeu choisies par le joueur, L'invention vise également à permettre la simulation d'un ou de plusieurs lancés de dés, en effectuant au sein du boîtier même, un tirage au sort des données de jeu qui seront comparées à des données de référence prédéterminées.

Un problème très important, inhérent à un tel dispositif de jeu, consiste à lutter contre la fraude. L'invention a à cet effet également

pour but, de prévoir plusieurs niveaux de sécurité et de vérification ayant trait aussi bien à l'origine du boîtier portable qu'au contenu de ses informations relatives d'une part à l'état "perdu" ou "gagné" du jeu, et d'autre part à la valeur proprement dite du gain accumulé par le joueur, valeur qui peut être très importante.

L'invention propose donc un dispositif électronique de jeu de hasard, comprenant

a) un boîtier portable comprenant

- une interface-boîtier d'entrée/sortie apte à recevoir une information prédéterminée d'autorisation de jeu sans laquelle le boîtier est inapte au jeu,

- une interface de communication avec le joueur,

- des moyens de mémoire aptes à stocker au moins une donnée de référence,

- des moyens de traitement-boîtier, comportant

. des moyens de comparaison aptes à comparer ladite donnée de référence avec une donnée de jeu introduite par le joueur par l'interface de communication, l'une de ces deux données étant une valeur générée de façon aléatoire,

. des moyens aptes à établir une information de gain dépendant au moins du résultat de ladite comparaison, et à stocker cette information de gain dans les moyens de mémoire, et

. des moyens de cryptage-boîtier, aptes en réponse à une information prédéterminée de demande de paiement reçue par l'interface-boîtier d'entrée/sortie, à établir une première valeur de gain cryptée à partir de ladite information de gain et à délivrer cette première valeur cryptée à l'interface-boîtier, et

b) un système de contrôle, externe au boîtier, comprenant

- une interface-système d'entrée/sortie apte à coopérer avec l'interface boîtier d'entrée/sortie, et

- des moyens de traitement-système, aptes,

. en présence d'une demande de paiement émanant du joueur, à lire ladite information de gain contenue dans les moyens de mémoire du boîtier et à délivrer ladite information de demande de paiement à l'interface-système d'entrée/sortie, et comportant

. des moyens de cryptage-système, homologues des moyens de cryptage-boîtier, aptes à établir une deuxième valeur de gain cryptée à partir de ladite information de gain lue, ainsi que des moyens de comparaison aptes à comparer les deux valeurs de gain cryptées; le paiement effectif du gain au joueur est alors conditionné au moins par la concordance des deux valeurs de gain cryptées.

L'homme du métier sait que le terme "aléatoire" associé ici à la génération d'une donnée de référence ou d'une donnée de jeu, est d'une façon générale un concept mathématique, et que la réalisation matérielle de moyens de génération "aléatoire" rendent cette génération pseudo ou quasi aléatoire, même si pratiquement il est impossible de prévoir à l'avance la donnée ayant été générée. Le terme "aléatoire" est néanmoins utilisé ici pour traduire l'impossibilité pratique, pour un tiers de prévoir à l'avance la donnée de jeu ou la donnée de référence.

Selon un mode de réalisation les moyens de traitement-système sont aptes à transmettre ladite information prédéterminée d'autorisation de jeu. Par ailleurs, afin de lire l'information de gain, les moyens de traitement-système sont aptes, en présence d'une demande de paiement émanant du joueur, à transmettre à l'interface - système d'entrée/sortie une demande de statut en réponse à laquelle les moyens de traitement-boîtier délivrent ladite information de gain à l'interface-boîtier d'entrée/sortie.

Selon un mode de réalisation les moyens de traitement-boîtier comportent des premiers moyens de génération aléatoire aptes à générer aléatoirement ladite donnée de référence parmi un ensemble prédéterminé de valeurs, tandis que l'interface de communication comporte des moyens d'introduction de données permettant au joueur de choisir sa donnée de jeu parmi le même ensemble prédéterminé de valeurs.

Afin d'assurer le caractère aléatoire du tirage au sort des données de référence, les premiers moyens de génération aléatoire comportent avantageusement au moins un compteur de jeu fonctionnant depuis un instant initial précédant la réception de ladite information prédéterminée d'autorisation de jeu, ce compteur étant susceptible

d'être stoppé à la réception d'une information d'arrêt choisie et de mémoriser la valeur qu'il présente lors de son arrêt de fonctionnement, cette valeur d'arrêt définissant, ladite donnée de référence.

L'information d'arrêt est de préférence ladite information d'autorisation de jeu.

En variante, il est possible de concevoir un jeu dans lequel les données de référence sont par exemple des constantes fixées par les règles du jeu, les données de jeu devant être choisies aléatoirement par le joueur d'une façon analogue à un lancé de dés. Dans une telle variante les moyens de traitement-boîtier peuvent comporter des deuxièmes moyens de génération aléatoire, commandés par l'action du joueur et aptes à délivrer aléatoirement ladite donnée de jeu, la donnée de référence étant une donnée prédéterminée stockée dans les moyens de mémoire.

Afin d'assurer une meilleure sécurité dans la vérification de l'information de gain, les moyens de mémoire sont aptes à stocker une première donnée auxiliaire prédéterminée, et les moyens de cryptage-boîtier sont aptes à générer la première valeur de gain cryptée à partir de ladite information de gain et de ladite première donnée auxiliaire.

La première donnée auxiliaire est avantageusement obtenue à partir d'un premier cryptage auxiliaire d'au moins une première information spécifique au boîtier telle que son numéro de série, et est présente dans les moyens de mémoire avant la réception de l'information d'autorisation de jeu.

Selon un mode de réalisation les moyens de cryptage-boîtier comportent:

un générateur pseudo-aléatoire de cryptage de gain apte à être initialisé par une valeur initiale et à fonctionner jusqu'à la réception d'une indication d'arrêt, la première valeur de gain cryptée étant alors la valeur délivrée par le générateur pseudo-aléatoire de cryptage de gain à la réception de ladite indication d'arrêt,

- un premier circuit logique apte à recevoir comme variables d'entrée ladite information de gain et une partie au moins de la première donnée auxiliaire stockée, à appliquer une première fonction logique prédéterminée à ces deux variables d'entrée et à délivrer une première

valeur de sortie correspondante, définissant ladite valeur initiale du générateur pseudo-aléatoire de cryptage de gain, et

- un compteur auxiliaire apte à compter ou décompter depuis une valeur initiale-compteur jusqu'à une valeur finale-compteur, ladite indication d'arrêt du fonctionnement du générateur pseudo-aléatoire de cryptage de gain étant délivrée par le compteur auxiliaire lorsque ladite valeur finale-compteur est atteinte.

Les moyens de cryptage-boîtier comprennent également de préférence un second circuit logique apte à recevoir comme variables d'entrée un mot binaire pseudo-aléatoire et une deuxième partie au moins de la première donnée auxiliaire stockée, à appliquer une deuxième fonction logique prédéterminée à ces deux variables d'entrée et à délivrer une deuxième valeur de sortie correspondante, définissant ladite valeur initiale compteur ou ladite valeur finale compteur.

Les moyens de traitement-système comportent avantageusement des moyens de génération pseudo-aléatoire-système aptes à générer ledit mot binaire pseudo-aléatoire, ce mot binaire pseudo-aléatoire accompagnant ladite information de demande de paiement.

Afin d'effectuer la vérification de la première valeur de gain cryptée, les moyens de traitement-système comportent des premiers moyens de cryptage auxiliaires aptes à effectuer ledit premier cryptage auxiliaire de ladite première information spécifique pour recalculer la valeur de la première donnée auxiliaire; par ailleurs, les moyens de cryptage-système comportent des moyens analogues à ceux des moyens de cryptage-boîtier, et sont aptes à déterminer la deuxième valeur de gain cryptée à partir de la valeur de la première donnée auxiliaire recalculée et du mot binaire pseudo-aléatoire. Cette deuxième valeur de gain cryptée sera alors comparée avec la première.

Afin d'effectuer une autre vérification avant paiement, les moyens de mémoire sont avantageusement aptes à stocker une deuxième donnée auxiliaire prédéterminée, et les moyens de traitement-système sont aptes, en présence de la demande de paiement émanant du joueur, à effectuer un traitement de vérification de la valeur de cette deuxième donnée auxiliaire, avant de délivrer ladite information de demande de paiement au boîtier. Cette deuxième donnée auxiliaire peut être un

certificat par un algorithme de codage à clé secrète ou publique d'un authentifiant spécifique au système de contrôle tel que le numéro de série d'un terminal de vente.

Afin de vérifier l'origine du boîtier il est avantageusement prévu que les moyens de mémoire soient aptes à stocker, avant la réception de ladite information d'autorisation de jeu, une donnée d'authentification du boîtier; la réception de ladite information d'autorisation de jeu est alors conditionnée à la vérification de cette donnée d'authentification.

Cette donnée d'authentification peut résulter d'un cryptage d'authentification d'une troisième information spécifique au boîtier; il peut s'agir d'un certificat du numéro de série du boîtier obtenu à partir d'un algorithme de cryptage à clé secrète ou publique utilisant une autre clé que celle prévue pour la deuxième donnée auxiliaire.

Les moyens de traitement-système comportent alors de préférence des moyens de cryptage d'authentification aptes à recalculer la donnée d'authentification à partir de la troisième information spécifique pour vérifier la valeur de cette troisième information spécifique lue dans les moyens de mémoire.

Le numéro de série du boîtier peut être présent dans les moyens de mémoire du boîtier. Il peut également être lu par un moyen de lecture approprié, par exemple par un lecteur optique si le numéro de série figure sous forme de code-barres sur une étiquette fixée sur le boîtier.

Selon un mode de réalisation les moyens de mémoire comportent deux mémoires, l'une d'entre elles contenant la première donnée auxiliaire, l'autre contenant d'abord la donnée d'authentification puis, après vérification de cette dernière, la deuxième donnée auxiliaire.

Par ailleurs les moyens de mémoire peuvent comporter un compteur d'état apte à contenir une information d'état représentative du résultat du jeu, ainsi qu'un compteur de paiement apte à contenir une information de paiement représentative d'un paiement déjà effectué ou non encore effectué au joueur.

En présence de la demande de paiement émanant du joueur, les moyens de traitement-système sont alors aptes à lire en outre les contenus des compteurs d'état et de paiement avant de délivrer ladite

information de demande de paiement au boîtier.

Le boîtier comporte avantageusement des moyens d'alimentation autorisant le fonctionnement de certains au moins de ces moyens, tels que les compteurs de jeu et les mémoires, avant la réception de l'information d'autorisation de jeu.

Le boîtier est avantageusement inapte au jeu à la suite d'une comparaison entre une donnée de référence et une donnée de jeu représentative d'un jeu perdant et/ou après un paiement effectif au joueur.

L'interface de communication comporte de préférence des moyens de restitution au joueur d'une information de résultat représentative du résultat de la comparaison entre les données de jeu et de référence, lui indiquant s'il a perdu ou gagné.

Selon un mode de réalisation de l'invention les moyens de mémoire sont aptes à stocker une pluralité de données de référence, et une pluralité de données de jeu sont susceptibles d'être introduites par le joueur.

Ces données de jeu peuvent être introduites successivement, chaque donnée de jeu introduite étant comparée à une donnée de référence prédéterminée; une donnée de jeu ne peut être introduite par l'interface de communication qu'en cas d'une concordance entre la donnée de jeu précédemment introduite et la donnée de référence correspondante, et à chaque concordance correspond une information de gain différente.

L'information de résultat comporte alors avantageusement l'affichage d'une information de niveau de gain correspondant à l'information de gain contenue dans les moyens de mémoire.

Les moyens de mémoire comportent de préférence un compteur de gain apte à contenir successivement des mots binaires de gain prédéterminés représentatifs des informations de gain successives, chaque mot binaire différant du mot suivant et du mot précédent par au moins deux bits. Ceci permet d'avoir des mots binaires suffisamment différents les uns des autres, afin de bien différencier les informations de gain correspondantes et d'éviter notamment des erreurs occasionnées par exemple par une mauvaise lecture ou écriture

d'un seul bit. De même le compteur d'état est avantageusement apte à contenir successivement des mots binaires d'état prédéterminés représentatifs des informations d'état successives, chaque mot binaire d'état différant du mot suivant et du mot précédent par au moins deux bits.

Lorsque plusieurs données de jeu doivent être introduites par le joueur, notamment successivement, les premiers moyens de génération aléatoire comportent de préférence une pluralité de compteurs de jeu, chaque compteur étant susceptible de contenir une donnée de référence et est associé à une introduction de donnée de jeu par le joueur. On peut alors prévoir que la réception de ladite information d'autorisation de jeu stoppe le fonctionnement de tous les compteurs, la pluralité de données de référence étant alors la pluralité de valeurs qu'avaient les compteurs à la réception de cette information d'autorisation de jeu. En d'autres termes, le tirage au sort des données de référence est effectué une fois pour toutes avant l'introduction des données de jeu par le joueur. On peut cependant prévoir qu'un tirage au sort s'effectue pour chaque donnée de jeu introduite. Dans ce cas un seul compteur peut être associé à toutes les introductions successives des données de jeu par le joueur; l'introduction d'une donnée de jeu par le joueur fige alors le compteur correspondant à une valeur définissant la valeur de référence associée à cette donnée de jeu.

Le système de contrôle comporte avantageusement une interface de dialogue avec le joueur apte à recevoir ladite demande de paiement. Cette interface de dialogue peut être utilisée à d'autres fins. Ainsi, en présence d'une demande de vérification d'information de gain émanant du joueur, les moyens de traitement-système peuvent lire les contenus des compteurs de gain, d'état, et de paiement et communiquer les résultats de cette lecture sur l'interface de dialogue.

Le système de contrôle peut comporter au moins une station, telle qu'un terminal, et de préférence une pluralité de stations de structure analogue, les informations d'autorisation de jeu et de demande de paiement pouvant être délivrées par la même station ou par deux stations différentes.

Afin d'effectuer une autre vérification, notamment lorsque le gain

est important, le système de contrôle comporte avantageusement des moyens de stockage d'une liste d'authentifiants des boîtiers gagnants et payés, et en présence d'une demande de paiement émanant du joueur et correspondant à un gain supérieur à une valeur de gain prédéterminée, les moyens de traitement-système sont aptes à vérifier si l'authentifiant du boîtier concerné se situe déjà dans ladite liste.

L'invention a également pour objet un boîtier et un système de contrôle appartenant à un tel dispositif électronique de jeu de hasard.

D'autres avantages et caractéristiques de l'invention apparaîtront à l'examen de la description détaillé d'un mode de réalisation nullement limitatif et illustré sur les dessins sur lesquels :

- la figure 1 représente schématiquement une station et un boîtier selon l'invention,
- la figure 2 illustre un réseau de stations,
- les figures 3a, 3b, 3c représentent plus en détail le boîtier de la figure 1,
- la figure 4 représente un écran d'affichage du boîtier,
- les figures 5, 6 et 7 représentent des synoptiques schématiques de l'architecture câblée d'un composant ASIC incorporé au boîtier, et
- les figures 8, 9, 10a, 10b, 10c représentent des organigrammes de fonctionnement du dispositif et de mise en oeuvre du jeu.

Tel qu'illustré sur la figure 1, le dispositif électronique de jeu comporte un boîtier portable 11 et un système de contrôle 12, externe au boîtier 11, et comprenant une interface-système d'entrée/sortie 17, comportant ici deux plages de cuivre 17a et 17b aptes à coopérer avec des plages cuivre homologues d'une interface-boîtier d'entrée/sortie du boîtier 11 afin de réaliser un échange de données par un couplage capacitif.

Outre cette interface d'entrée/sortie 17, le système de contrôle 12 comporte des moyens de traitement-système 16 connectés à cette interface 17 ainsi qu'à une interface de dialogue 13 avec un utilisateur tel que le vendeur ou l'agent payeur. Cette interface de dialogue comporte un écran d'affichage 14 ainsi qu'un clavier 15 pour l'introduction d'informations de commande par exemple.

Les moyens de traitement-système 16 sont incorporés au sein

d'une carte électronique architecturée autour d'un micro-contrôleur dialoguant avec l'interface 17 par l'intermédiaire d'un registre d'entrée/sortie 88. Comme on le verra plus en détails ci-après lors du fonctionnement du dispositif, les moyens de traitement-système 16 comportent des moyens de cryptage-système 19, des premier et deuxième moyens de cryptage auxiliaires 20a et 20b, des moyens de cryptage d'authentification 21 ainsi que des moyens de génération pseudo-aléatoire système 22 aptent à générer un mot binaire pseudo-aléatoire dont la signification sera expliquée ci-après. Matériellement, ces différents moyens sont réalisés de façon logicielle au sein du micro-contrôleur des moyens de traitement-système.

Sur la figure 1, les moyens de traitement-système 16, l'interface-système d'entrée/sortie 17 et l'interface de dialogue 13 sont matériellement regroupés au sein d'une station telle qu'un terminal. On peut à cet effet prévoir d'utiliser un micro-ordinateur classique, tel que par exemple celui connu sous la marque PC de la société IBM. Dans ce cas, l'interface de dialogue 13 comportera l'écran et le clavier du micro-ordinateur. On peut alors prévoir une carte électronique supplémentaire enfichable dans le micro-ordinateur et incorporant les moyens de traitement-système, ainsi qu'une extension réalisant l'interface 17.

Bien que d'une façon générale, le système de contrôle puisse être incorporé au sein d'une seule station, il est prévu d'utiliser un réseau de stations 12 (figure 2) ayant toutes une structure analogue. Certaines au moins de ces stations peuvent être reliées à des moyens de stockage 23 aptent à stocker, comme on le verra plus en détails ci-après, une liste d'authentifiants de boîtiers ayant abouti à un jeu gagnant et ayant donné lieu à un paiement effectif au joueur.

Le boîtier 11 a des dimensions hors tout lui permettant de tenir aisément dans une main. Il comporte sur sa face avant (figure 3a) une touche 24 permettant de le mettre sous tension pour activer certains au moins des moyens le constituant, comme par exemple l'écran d'affichage 28. Par ailleurs, il est prévu, dans cet exemple de réalisation trois touches de jeu 25, 26 et 27, sur lesquelles sont respectivement inscrits trois chiffres (1, 2 et 3) représentant trois

données de jeu parmi lesquelles le joueur pourra faire son choix.

Sur sa face arrière (figure 3c) se trouve une étiquette sur laquelle figure par exemple en code barre, le numéro de série NS du boîtier. Ce numéro de série constitue ici un authentifiant unique et spécifique au boîtier.

La figure 3b illustre schématiquement une vue interne du boîtier 11. On y trouve les empreintes électroniques 21, 32, 33 et 34 des touches 24, 25, 26 et 27. Deux plages de cuivre 29 et 30, faisant partie d'une interface-boîtier d'entrée/sortie, sont aptes à coopérer avec les deux plages de cuivre homologues 17a et 17b d'une station 12. Des moyens d'alimentation autonomes 35 et 36, tels que les piles, permettent d'assurer le caractère autonome du boîtier portable et servent, comme on le verra ci-après, à alimenter de façon permanente certains des composants du boîtier.

Alors que les trois touches de jeu 25, 26, 27 et l'écran d'affichage 28 forment une interface de communication avec le joueur, un élément essentiel de l'invention consiste ici en un circuit intégré câblé spécifique (ASIC: Application Specific Integrated Circuit) portant la référence 37 et incorporant comme on le verra plus en détails ci-après, des moyens de traitement-boîtier ainsi que des moyens de mémoire. Cet ASIC est relié par un réseau de connexion 38 aux touches de jeu, aux moyens d'alimentation, ainsi qu'à l'écran d'affichage 28. Bien entendu, on aurait pu utiliser, à la place d'un composant ASIC, un micro-contrôleur incorporant de façon logicielle certaines au moins des fonctions du boîtier qui seront décrites ci-après. Néanmoins, l'utilisation d'un composant ASIC permet de réduire les coûts de fabrication et augmente la sécurité du dispositif selon l'invention, contre la fraude. Il est en effet plus difficile, pour un fraudeur, d'accéder et de comprendre l'architecture d'un schéma de câblage spécifiquement réalisé pour une application et incorporé au sein d'un ASIC, que d'accéder aux instructions d'un programme incorporé au sein d'une mémoire de programme d'un micro-contrôleur.

Sur la figure 4, est représenté un écran d'affichage 28 tel qu'il est susceptible d'apparaître au joueur dans l'application spécifique de jeu qui est décrite dans cet exemple. En bas de l'écran d'affichage sont

prévus deux espaces GA et FI dans lesquels sont susceptibles d'être affichés les expressions "GAGNE" et "FIN" selon que le joueur a gagné ou perdu dans son jeu de hasard. Sur les deux bords latéraux de l'écran d'affichage sont disposés respectivement deux colonnes d'emplacements numérotés 1, 2, 3, 4, 5 et 6, 7, 8, 9, 10. Ces emplacements portent les références NG1-NG10 et correspondent à des affichages de niveaux de gains successifs atteints par le joueur lors de son jeu. Au centre de l'écran d'affichage, figurent des emplacements pour trois flèches F respectivement positionnées en regard d'emplacements circulaires N1, N2 et N3 à l'intérieur desquels sont matérialisés les trois chiffres 1, 2 et 3. Comme on le verra ci-après, l'une de ces flèches F va matérialiser le choix du joueur après que celui-ci ait appuyé sur l'une des touches de jeu 25 à 27, tandis que l'un des emplacements N1, N2 ou N3 matérialisera la donnée de référence tirée au hasard par le boîtier lui-même.

La figure 5 représente schématiquement une partie des moyens incorporés au sein du composant 37. On trouve tout d'abord un registre d'entrée-sortie série/parallèle 39, faisant partie de l'interface-boîtier d'entrée/sortie, et relié aux deux plages de cuivre 29 et 30. A ce registre 39 est relié un circuit décodeur 40 apte à décoder les diverses informations reçues par le registre 39 (entrée/sortie, écriture, lecture). Ce circuit décodeur 40 est relié à un circuit de mise en forme 51, connecté en premier lieu à un compteur d'état 48, tel qu'un compteur non linéaire, susceptible de contenir une information d'état représentative du résultat "perdu" ou "gagné" du jeu, en deuxième lieu à un compteur 49 susceptible de contenir une information représentative d'un paiement ayant été réellement effectué au joueur, et en troisième lieu à un compteur dit de gain 50, tel qu'un compteur non linéaire, apte à contenir une information de gain dépendant du résultat du jeu. En réponse à une demande de statut, le circuit de mise en forme est apte à délivrer au registre d'entrée/sortie 39 les contenus C1, C2, C3 des trois compteurs précités 48, 49 et 50.

La sortie du compteur de gain 50 est également reliée à l'entrée d'un premier circuit logique 47 dont l'autre entrée est reliée à une première mémoire vive M1. La sortie du premier circuit logique est

reliée à un générateur pseudo-aléatoire dit de cryptage de gain 46, tel qu'un compteur polynomial ou un générateur cyclique, commandé également par un compteur auxiliaire 45 recevant en entrée la sortie d'un deuxième circuit logique 44 dont les deux entrées sont respectivement reliées à la mémoire M1 et au registre d'entrée sortie 39. La sortie du générateur pseudo-aléatoire de cryptage de gain 46 est reliée au registre 39.

Il est également prévu des moyens de contrôle logiques 41 de l'ensemble de ces moyens, cadencés par un signal d'horloge CLK d'une fréquence par exemple de 500 kHz, délivré par un oscillateur 43.

Une autre mémoire vive M2, reliée au registre d'entrée-sortie 39 fait partie, avec la mémoire M1, des moyens de mémoire du boîtier.

Les figures 6 et 7 illustrent plus en détail des premiers moyens de génération aléatoire aptes à générer les données de référence qui seront comparées avec les données introduites par le joueur.

La figure 6 est représentative d'un mode de réalisation applicable à un tirage au sort, effectué une seule fois pour une pluralité de données de référence successives (dix par exemple) correspondant respectivement à des introductions potentielles successives de données de jeu par le joueur.

Une porte logique ET 52 reçoit en entrée le signal d'horloge CLK ainsi qu'une information d'autorisation de jeu DV dont on reviendra ultérieurement plus en détail sur la signification. La sortie de cette porte logique 52 est relié au premier compteur modulo 2 (53-1) d'une rangée de dix compteurs 53-1 à 53-10 reliés en cascade les uns aux autres et dont les sorties sont respectivement reliées aux dix entrées d'un multiplexeur 54 dont la sortie est reliée à la première entrée d'un comparateur 55. Chaque compteur est donc susceptible d'afficher un contenu correspondant à l'un des trois chiffres 1, 2 et 3. Ce multiplexeur 54 est commandé en ce qui concerne le choix de sa voie d'entrée par la sortie du compteur de gain 50. L'autre entrée du comparateur 55 reçoit la valeur VJ de la donnée de jeu introduite par le joueur. La sortie de ce comparateur est reliée au compteur d'état 58 et au compteur de gain 50.

Comme on le verra ci-après, la figure 7 illustre un mode de

réalisation plus particulièrement adapté, soit à des tirages au sort successifs associés respectivement aux introductions successives des données de jeu par le joueur, soit à une génération aléatoire d'une donnée de jeu qui serait analogue par exemple à un lancé de dé de la part du joueur. Dans ce dernier cas, la donnée de référence qui sera comparée avec la donnée de jeu générée aléatoirement, pourra être une constante mémorisée dans les moyens de mémoire du boîtier. Sur ce mode de réalisation, la porte logique 52 reçoit à la place de l'information d'autorisation de jeu DV le signal d'introduction ACJ d'une donnée de jeu par le joueur sur l'interface de communication. Il n'est alors prévu qu'un seul compteur 53 relié à cette porte logique 52 et dont la sortie est reliée à la première entrée du comparateur 55.

On va maintenant décrire plus en détails, en se référant plus particulièrement aux figures 8 à 10c le fonctionnement du dispositif selon l'invention.

Lors de la fabrication en usine (étape 56) une première donnée auxiliaire IC1 est inscrite dans la mémoire M1 tandis qu'une donnée d'authentification IC2 est inscrite dans la mémoire M2 (étape 57 et étape 58). La première donnée auxiliaire IC1 constitue une première sécurité qui sera utilisée lors du paiement effectif du gain au joueur. Elle résulte d'une façon générale d'un premier cryptage auxiliaire d'une information spécifique au boîtier. Plus précisément, il s'agit par exemple d'une information cryptée obtenue à partie du numéro de série NS du boîtier par un algorithme de cryptage du type à clef secrète, tel que celui connu sous le sigle DES (Data Encryption Standard) et utilisant à cet effet une première clef secrète. Il serait également possible d'utiliser un algorithme de cryptage à clé publique tel que celui connu sous le sigle RSA (Rivest Shamir Adelman).

La donnée d'authentification IC2 consiste également en un cryptage d'authentification d'une information spécifique du boîtier. Concrètement, il s'agit d'un cryptage du numéro de série du boîtier à partir d'un algorithme à clef secrète (ou éventuellement publique), avec une clef différente de celle utilisée pour l'information IC1. Cette donnée IC2 est en fait un certificat du numéro de série NS.

Afin de préserver les contenus des mémoires vives M1 et M2, le

boîtier sera alimenté par ses moyens d'alimentation en permanence depuis sa fabrication en usine. De ce fait, lesdits compteurs 53-1 à 53-10 fonctionnent depuis le stade de fabrication du boîtier en usine.

Néanmoins, à ce stade, le boîtier est inapte au jeu ou verrouillé. En d'autres termes, les moyens de traitement-boîtier sont inactifs et un joueur, qui viendrait à être en possession d'un tel boîtier, ne pourrait pas introduire de données de jeu à l'aide des touches 25-27.

A sa sortie d'usine, le boîtier est stocké dans un local de vente équipé d'une station de contrôle 12. Lors de la vente d'un tel boîtier à un joueur, il est tout d'abord procédé à une validation de celui-ci (étape 59). Le boîtier étant disposé sur l'interface-système 17, les moyens de traitement-système 16 procèdent à une lecture du contenu de la mémoire M2, et les moyens de cryptage d'authentification 21 recalculent, à partir du numéro de série NS et de la valeur de la clef secrète utilisée (présente également dans des moyens de mémoire de la station), la donnée d'authentification IC2. A cet effet, les moyens de traitement-système peuvent avoir connaissance du numéro de série NS du boîtier soit en raison de son stockage directement dans la mémoire M2 du boîtier, soit par une lecture optique à l'aide d'un lecteur approprié, du code barre situé sur la face arrière du boîtier. La concordance de la donnée de d'authenfication recalculée avec celle qui était présente dans la mémoire M2 avant cette étape de validation 59, permet d'effectuer une première vérification sur l'origine du boîtier et de s'assurer ainsi qu'il s'agit à priori d'un boîtier authentique.

Une fois cette vérification sur l'origine effectuée,les deuxièmes moyens de cryptage auxiliaire 20b des moyens de traitement-système déterminent une deuxième donnée auxiliaire cryptée IC3 à partir également d'une information spécifique à la station effectuant la vente et d'un algorithme de cryptage à clef secrète (ou éventuellement publique) utilisant une troisième clef différente des deux premières. Pratiquement, les deuxièmes moyens de cryptage auxiliaires utilisent comme information spécifique-station, son numéro de série, la date de la vente ainsi que le numéro d'ordre de cette vente à cette date, et déterminent le certificat crypté de cette information spécifique-station. Les moyens de traitement-système stockent alors dans la mémoire M2,

cette information spécifique-station ainsi que le certificat IC3.

La concordance de la donnée d'authentification IC2 stockée dans la mémoire M2, avec celle recalculée, a également pour conséquence l'émission par les moyens de traitement-système de la station, de l'information d'autorisation de jeu DV qui a pour effet d'une part d'activer les moyens de traitement-boîtier pour rendre le boîtier apte au jeu, et, d'autre part, de stopper le fonctionnement des compteurs de jeu 53-1 à 53-10. Cette information d'autorisation de jeu ainsi que la demande de statut sont en fait des commandes particulières émises par la station, et à la réception desquelles les moyens de traitement-boîtier effectuent des opérations prédéterminées. Il convient de remarquer que, dans ce mode de réalisation, la pluralité de données de référence est alors la pluralité de valeurs qu'avaient les compteurs 53-1 à 53-10 à la réception de l'information de d'autorisation de jeu. Ces données de référence sont mémorisées dans les compteurs 53-1 à 53-10 en vue de leur comparaison avec les données de jeu. Le tirage au sort de toutes les données de référence a donc été effectué une seule fois. Par ailleurs, la cadence rapide de fonctionnement des compteurs ainsi que le caractère aléatoire de l'instant de mise en marche des compteurs à l'usine de fabrication et de l'instant de réception de l'information DV contribuent au caractère "aléatoire" de la génération des données de référence.

Bien entendu, dans la variante illustrée sur la figure 7, concernant des tirages au sort successifs de données de référence, la réception de l'information d'autorisation de jeu DV n'a pour seul effet que l'activation des moyens de traitement de boîtier, et le déverrouillage de celui-ci afin de le rendre apte au jeu.

Le joueur est maintenant en possession d'un boîtier avec lequel il peut jouer.

La phase de jeu proprement dite 60, correspondant ici à un exemple bien particulier de jeu, est illustrée plus en détail sur la figure 9. Lors de la mise en marche du boîtier (étape 61) par pression sur la touche 24, l'écran 28 affiche (étape 62) les chiffres 1, 2 et 3 dans les emplacements N1, N2 et N3 ainsi que le niveau de gain antérieur. Si le joueur n'a jamais joué avec ce boîtier, il n'y a bien

entendu aucun affichage de niveau de gain antérieur.

Dans l'étape 63, le joueur choisi un chiffre et actionne la touche 25-27 correspondante ce qui matérialise l'introduction de sa donnée de jeu. La flèche F, en regard de l'emplacement N1, N2 ou N3 correspondant au chiffre choisi par le joueur, s'affiche et les moyens de traitement-boîtier activent alors un logiciel d'animation visuelle, communément appelé "chenillard" par l'homme du métier, et ayant pour effet de provoquer une rotation, sur l'écran d'affichage 28 des chiffres 1, 2 et 3 simulant ainsi le mouvement d'une roulette dans un jeu de roulette. Le chenillard simule ensuite la décélération de la roulette et le chiffre correspondant à la donnée de référence contenue dans le premier compteur de jeu 53-1 s'affiche à l'emplacement correspondant sur l'écran d'affichage 28 (étapes 64, 65).

Si le chiffre s'affiche en face de la flèche F qui matérialisait la donnée de jeu choisie par le joueur (étape 67), celui-ci a gagné. Dans ce cas, l'expression "GAGNE" s'affiche à l'emplacement GA et le niveau de gain 1 s'affiche à l'emplacement NG1. Dans le cas contraire (étape 66), c'est-à-dire si le chiffre correspondant à la donnée de référence ne s'affiche pas en regard de la flèche F, le joueur a perdu et l'expression "FIN" s'affiche dans l'emplacement FI. Dans un tel cas, les moyens de traitement-boîtier verrouillent (étape 68) l'interface de communication avec le joueur en ce sens que celui-ci ne peut plus introduire de donnée de jeu à l'aide des touches 25-27. En d'autres termes, le boîtier est rendu à nouveau inapte au jeu et peut être jeté par exemple.

Dans le cas d'un jeu gagnant, le joueur à deux possibilités. Soit il décide d'arrêter de jouer et de demander le paiement de son gain en se présentant à une station 12, soit il décide de tenter sa chance une nouvelle fois en choisissant à nouveau une donnée de jeu qu'il introduit à l'aide des touches 24-27. Le déroulement du jeu s'effectue alors à nouveau selon les étapes 63 à 66 ou 67. Dans le mode de réalisation illustré sur la figure 6, le contenu du compteur de gain, permet de sélectionner la voie d'entrée du multiplexeur 54 puisque ce compteur de gain comporte une information de gain différente pour chaque essai gagnant du joueur. Aussi, dans le cas présent, lors du

deuxième essai, le deuxième compteur 53-2 de la chaîne sera sélectionné et son contenu correspondant à la deuxième valeur de référence sera comparé à la donnée de jeu introduite par le joueur. Le joueur peut ainsi tenter sa chance dix fois de suite pour espérer atteindre le niveau de gain 10. A chaque nouvel essai gagnant, son niveau de gain actuel s'affiche et est supérieur au niveau de gain précédent. Par contre, si au cours de ce cheminement, un essai devient perdant, le boîtier devient inapte au jeu et le niveau de gain précédent reste affiché. Bien entendu, le joueur ne peut tenter un essai suivant que s'il a réussi à l'essai précédent, c'est à dire si il y avait concordance entre la donnée de référence associée à son essai précédent et la donnée de jeu qu'il avait alors introduite.

Dans le mode de réalisation illustré sur la figure 7, les dix données de référence correspondant aux dix niveaux de gain ne sont pas prédéterminées à l'avance. Le compteur 53 fonctionne jusqu'à l'actionnement d'une touche 24-27 par le joueur matérialisant son choix d'une donnée de jeu. Cette action ACJ bloque alors le compteur 53 à une valeur définissant à la valeur de référence générée aléatoirement et associée à l'introduction de la donnée de jeu par le joueur lors de son essai. Après l'affichage d'un résultat gagnant éventuelle, le fonctionnement du compteur 53 se poursuit et celui-ci sera à nouveau figé à une autre valeur lors de l'introduction éventuelle ultérieure d'une autre donnée de jeu par le joueur.

La variante de la figure 7 est également compatible avec un autre type de jeu consistant cette fois ci à comparer des données de référence constantes prédéterminées et stockées en mémoire, avec des données de jeu introduites de façon aléatoire par le joueur. On simule ainsi un lancement de dés par le joueur. Dans ce cas, la réception du signal à ACJ, provoqué par l'actionnement d'une touche appropriée sur le boîtier par le joueur, provoque l'arrêt du compteur 53 matérialisant la génération aléatoire de la donnée de jeu qui sera ensuite comparée à la valeur de référence (désignée ici également par VJ) stockée en mémoire.

Dans le cas où un joueur ayant gagné et ayant atteint un certain niveau de gain, décide de ne plus jouer et de demander le paiement de

ce gain, il procède alors à une demande de paiement 69 auprès d'une station 12 qui va procéder alors à une phase de vérification approfondie 70. Il convient de noter ici que le joueur peut demander ce paiement auprès de la même station qui lui a vendu son boîtier ou auprès d'une station homologue.

On se réfère maintenant plus particulièrement aux figures 10a à 10c pour décrire cette phase de vérification.

Celle-ci commence tout d'abord par une vérification visuelle 71 de la part de l'agent chargé d'effectuer le paiement. Cette vérification visuelle consiste à vérifier l'affichage de l'expression "GAGNE" ainsi que l'affichage d'un niveau de gain. Si aucune anomalie 72 n'apparaît, le boîtier est alors placé sur l'interface 17 d'entrée-sortie de la station et les moyens de traitement-système délivrent au moyen de traitement-boîtier une demande de statut (étape 73). A la réception 74 de cette demande de statut ST1, les moyens de traitement-boîtier délivrent au registre d'entrée-sortie 39 les contenus respectifs C1, C2, C3 des compteurs 48, 49 et 50, ainsi que le contenu de la mémoire M2. Les contenus respectifs C1, C2, C3 sont alors affichés en "clair" sur l'écran 14 de l'interface de dialogue de la station (étape 78). Ceci constitue une autre vérification visuelle qui cependant ne fait pas foi pour le paiement effectif du gain au joueur, comme cela sera expliqué ci-après.

On passe ensuite à une étape de vérification 81 consistant à vérifier la valeur de la deuxième donnée auxiliaire IC3 contenue dans la mémoire M2. Pour celà, les deuxièmes moyens de cryptage auxiliaire 20b des moyens de traitement-système de la station lisent l'information spécifique-station (numéro de série de la station, date de la vente et numéro d'ordre) dans la mémoire M2, et recalculent le certificat IC3 de cette information spécifique pour le comparer à celui contenu dans la mémoire M2.

Une non concordance de ces deux données IC3 conduit encore à une anomalie 82 qui peut interrompre le processus de paiement. Dans le cas contraire, les moyens de traitement-système comparent l'information de gain du compteur de gain 50 à une valeur de gain prédéterminée GS. Si le gain est supérieur à cette valeur GS, les

moyens de traitement-système vérifient alors si l'authentifiant du boîtier concerné , c'est à dire son numéro de série, ne se situe pas déjà dans la liste d'authentifiants des boîtiers gagnants et déjà payés. Si tel était le cas, il y aurait encore une anomalie 85 interrompant le processus de paiement. Si la station 12 n'est pas reliée aux moyens de stockage 23 de cette liste, le joueur est prié alors de se rendre auprès d'une station reliée à cette liste. Bien entendu, le joueur peut être prié de changer de station juste après la vérification visuelle 71.

Dans le cas où, soit le gain est inférieur à la valeur GS, soit le gain est supérieur à la valeur GS et le boîtier ne se situe pas dans la liste gagnante, les moyens de traitement-système émettent alors (étape 86) une information de demande de paiement IDP accompagnée d'un mot binaire aléatoire MBA. A la réception 87 de l'information IDP et du mot binaire MBA, par l'interface d'entrée-sortie du boîtier, les moyens de cryptage (44, 45, 46, 47) du boîtier sont aptes à générer une première valeur de gain cryptée VF1 à partir de l'information de gain contenue dans le compteur de gain 50 et de la première donnée auxiliaire IC1 contenue dans la mémoire M1 (étapes 88-92).

Pour celà, le générateur pseudo-aléatoire de cryptage de gain 46 est apte à être initialisé par une valeur initiale et à fonctionner jusqu'à la réception d'une indication d'arrêt. La première valeur de gain cryptée VF1 est alors la valeur délivrée par le générateur pseudo-aléatoire de cryptage de gain 46 à la réception de cette indication d'arrêt.

Le premier circuit logique 47 reçoit comme variable d'entrée l'information de gain contenue dans le compteur de gain 50 et une partie de la première donnée auxiliaire IC1 stockée dans la mémoire M1. Ce premier circuit 47 applique alors une première fonction logique prédéterminée, par exemple à base de OU exclusif, à ces deux variables d'entrée et délivre une première valeur de sortie correspondante, qui définie la valeur initiale du générateur pseudo-aléatoire de cryptage de gain 46.

Le compteur auxiliaire 45 est apte à compter ou décompter depuis une valeur initiale-compteur jusqu'à une valeur finale-compteur. L'indication d'arrêt du fonctionnement du générateur pseudo-aléatoire

de cryptage de gain est alors délivré par le compteur auxiliaire 45 lorsque ladite valeur finale-compteur est atteinte.

Le deuxième circuit logique 44 est utilisé ici pour définir la valeur initiale compteur ou la valeur finale compteur selon que le compteur compte ou décompte.

Ce deuxième circuit logique reçoit comme variables d'entrée le mot binaire pseudo-aléatoire MBA et une deuxième partie de la première donnée auxiliaire stockée IC1. Une deuxième fonction logique prédéterminée, de préférence différente de la première, est alors appliquée à ces deux variables d'entrée et le deuxième circuit logique 44, délivre une deuxième valeur de sortie qui définit la valeur initiale-compteur ou la valeur finale-compteur.

Ainsi, le compteur polynominal (par exemple) 46 est initialisé à une valeur initiale dépendant du contenu crypté de la mémoire M1 et de l'information de gain contenue dans le compteur de gain 50. Ce compteur fonctionnera alors jusqu'à ce que le compteur auxiliaire 45 s'arrête, le nombre d'itérations de ce dernier étant défini de façon pseudo-aléatoire à l'aide du mot binaire MBA. Lors de l'arrêt du compteur 46, son contenu, définissant la première valeur de gain cryptée VF1, est délivré aux moyens de traitement-système de la station par l'intermédiaire du registre d'entrée-sortie 39 étapes 93, 94).

Le paiement effectif du gain au joueur ne sera effectué que si cette première valeur de gain cryptée VF1 délivrée par le boîtier, est identique à une deuxième valeur de gain cryptée VF2 établie par les moyens de cryptage-système 19 de la station. A cet effet, les premiers moyens de cryptage auxiliaire 20a de la station recalculent la première donnée auxiliaire cryptée IC1 à partir du numéro de série du boîtier et de la clef secrète correspondante. Ce numéro de série peut être stocké dans la mémoire M1 ou bien lu optiquement par un lecteur optique. A partir de là, les moyens de cryptage-système, comportant des moyens analogues à ceux des moyens de cryptage-boîtier (c'est à dire des circuits logiques et des compteurs analogues aux circuites logiques 44, 47 et aux compteurs 45 et 46), calculent la deuxième valeur de gain cryptée, d'une façon analogue à celle utilisée pour le calcul de la première valeur de gain cryptée VF1, à partir de l'information IC1

recalculée par les premiers moyens de cryptage auxiliaires, et du mot binaire pseudo-aléatoire MBA qui est connu de la station puisque généré par les moyens de génération pseudo-aléatoire-système 22.

En cas de non concordance il y a de nouveau anomalie interrompant le processus de paiement. Par contre, en cas de concordance, le paiement 99 du gain est effectué au joueur, le boîtier est verrouillé (étape 101), le compteur 49 est chargé par une information représentative d'un paiement effectué au joueur et un archivage du numéro de série de ce boîtier gagnant est effectué (étape 100) soit au niveau de la station elle-même soit au niveau des moyens de stockage 23 notamment s'il s'agit d'un gain supérieur à la valeur GS.

Le conditionnement du paiement effectif du gain au joueur par la concordance des deux valeurs de gain cryptées VF1 et VF2 garantit l'organisme payeur contre la fraude provenant notamment de boîtiers falsifiés contenant des micro-processeurs programmés pour simuler des valeurs factices d'information de gain.

Bien que les autres étapes de vérification (demande de statut, vérification des données IC2 et IC3) ne soient pas indispensables, elles contribuent avantageusement à augmenter la sécurité contre la fraude. Par ailleurs, l'homme du métier aura compris que seul le contenu des compteurs 48, 49 et 50 fait foi vis-à-vis de l'organisme payeur, l'affichage de leur contenu sur l'écran 14 ou 28 n'étant qu'une indication visuelle. Aussi, toujours dans le but d'augmenter la sécurité, il est avantageusement prévu que le compteur de gain 50 soit agencé pour contenir successivement des mots binaires de gain prédéterminés représentatifs des informations de gain successives que pourrait obtenir le joueur s'il gagnait successivement à chaque essai. Chaque mot binaire diffère alors du mot précédent et du mot suivant dans la liste par au moins deux bits. Une telle précaution complexifie encore la tâche d'un fraudeur qui souhaiterait modifier le contenu du compteur de gain car il aurait à modifier deux bits à la fois et non un.

La même précaution peut être avantageusement utilisée pour le compteur d'état 48 avec une deuxième liste prédéterminée de mots binaires différant les uns des autres par au moins deux bits. Ceci

apporte en plus une double sécurité pour vérifier le niveau de gain obtenu et l'état perdu ou gagnant du jeu à chaque essai.

Enfin, il est possible qu'un joueur désire acheter un boîtier à une tierce personne pour continuer le jeu. Dans ce cas, il est particulièrement avantageux que l'acheteur puisse vérifier le contenu du compteur de gain notamment. Aussi, en présence d'une demande de vérification d'information de gain émanent du joueur acheteur, les moyens de traitement-système sont aptes à lire les contenus des compteurs de gain, d'état et de paiement et à communiquer les résultats de cette lecture sur l'écran 14 de l'interface de dialogue. Bien entendu, dans ce cas, l'information de demande de paiement IDP n'est pas délivrée au boîtier.

REVENDICATIONS

1. Dispositif électronique de jeu de hasard, comprenant

a) un boîtier portable (11) comprenant

- une interface-boîtier d'entrée/sortie (39, 29, 30) apte à recevoir une information prédéterminée d'autorisation de jeu sans laquelle le boîtier est inapte au jeu,

- une interface de communication (24, 25, 26, 27, 28) avec le joueur,

- des moyens de mémoire (M1, M2, 53-1,... 53-10, 48, 49, 50) aptes à stocker au moins une donnée de référence,

- des moyens de traitement-boîtier, comportant

. des moyens de comparaison (55) aptes à comparer ladite donnée de référence avec une donnée de jeu introduite par le joueur par l'interface de communication, l'une de ces deux données étant une valeur générée de façon aléatoire,

. des moyens (50) aptes à établir une information de gain dépendant au moins du résultat de ladite comparaison, et à stocker cette information de gain dans les moyens de mémoire (50), et

. des moyens de cryptage-boîtier (44-47), aptes en réponse à une information prédéterminée de demande de paiement (IDP) reçue par l'interface-boîtier d'entrée/sortie, à établir une première valeur de gain cryptée (VF1) à partir de ladite information de gain et à délivrer cette première valeur cryptée à l'interface-boîtier, et

b) un système de contrôle (12), externe au boîtier (11), comprenant

- une interface-système d'entrée/sortie (17) apte à coopérer avec l'interface boîtier d'entrée/sortie, et

- des moyens de traitement-système (16), aptes,

. en présence d'une demande de paiement émanant du joueur, à lire ladite information de gain contenue dans les moyens de mémoire du boîtier et à délivrer ladite information de demande de paiement (IDP) à l'interface-système d'entrée/sortie, et comportant

. des moyens de cryptage-système (19), homologues des moyens de cryptage-boîtier, aptes à établir une deuxième valeur de

gain cryptée (VF2) à partir de ladite information de gain lue, ainsi que des moyens de comparaison aptes à comparer les deux valeurs de gain cryptées,

le paiement effectif du gain au joueur étant conditionné au moins par la concordance des deux valeurs de gain cryptées.

2. Dispositif selon la revendication 1 caractérisé par le fait que les moyens de traitement-système sont aptes à transmettre ladite information prédéterminée d'autorisation de jeu (DV).

3. Dispositif selon la revendication 1 ou 2, caractérisé par le fait que les moyens de traitement-boîtier comportent des premiers moyens de génération aléatoire (53-1,... 53-10) aptes à générer aléatoirement ladite donnée de référence parmi un ensemble prédéterminé de valeurs, tandis que l'interface de communication comporte des moyens d'introduction de données (25-27) permettant au joueur de choisir sa donnée de jeu parmi le même ensemble prédéterminé de valeurs.

4. Dispositif selon la revendication 3, caractérisé par le fait que les premiers moyens de génération aléatoire comportent au moins un compteur de jeu (53-1,... 53-10) fonctionnant depuis un instant initial précédant la réception de ladite information prédéterminée d'autorisation de jeu (DV), ce compteur étant susceptible d'être stoppé à la réception d'une information d'arrêt choisie (DV) et de mémoriser la valeur qu'il présente lors de son arrêt de fonctionnement, cette valeur d'arrêt définissant, ladite donnée de référence.

5. Dispositif selon la revendication 4, caractérisé par le fait que l'information d'arrêt est ladite information d'autorisation de jeu (DV).

6. Dispositif selon la revendication 1 ou 2, caractérisé par le fait que les moyens de traitement-boîtier comportent des deuxièmes moyens de génération aléatoire (53), commandés par l'action du joueur et aptes à délivrer aléatoirement ladite donnée de jeu, la donnée de référence étant une donnée prédéterminée stockée dans les moyens de mémoire.

7. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les moyens de mémoire (M1) sont aptes à stocker une première donnée auxiliaire prédéterminée, (IC1),

et par le fait que les moyens de cryptage-boîtier (44-47) sont aptes à

générer la première valeur de gain cryptée (VF1) à partir de ladite information de gain et de ladite première donnée auxiliaire (IC1).

8. Dispositif selon la revendication 7, caractérisé par le fait que la première donnée auxiliaire est obtenue à partir d'un premier cryptage auxiliaire d'au moins une première information (NS) spécifique au boîtier, et est présente dans les moyens de mémoire (M1) avant la réception de l'information d'autorisation de jeu (DV).

9. Dispositif selon la revendication 7 ou 8, caractérisé par le fait que les moyens de cryptage-boîtier comportent:

- un générateur pseudo-aléatoire de cryptage de gain (46) apte à être initialisé par une valeur initiale et à fonctionner jusqu'à la réception d'une indication d'arrêt, la première valeur de gain cryptée (VF1) étant alors la valeur délivrée par le générateur pseudo-aléatoire de cryptage de gain à la réception de ladite indication d'arrêt,
- un premier circuit logique (47) apte à recevoir comme variables d'entrée ladite information de gain et une partie au moins de la première donnée auxiliaire stockée (IC1), à appliquer une première fonction logique prédéterminée à ces deux variables d'entrée et à délivrer une première valeur de sortie correspondante, définissant ladite valeur initiale du générateur pseudo-aléatoire de cryptage de gain, et
- un compteur auxiliaire (45) apte à compter ou décompter depuis une valeur initiale-compteur jusqu'à une valeur finale-compteur, ladite indication d'arrêt du fonctionnement du générateur pseudo-aléatoire de cryptage de gain (46) étant délivrée par le compteur auxiliaire lorsque ladite valeur finale-compteur est atteinte.

10. Dispositif selon la revendication 9, caractérisé par le fait que les moyens de cryptage-boîtier comprennent un second circuit logique (44) apte à recevoir comme variable d'entrée un mot binaire pseudo-aléatoire (MBA) et une deuxième partie au moins de la première donnée auxiliaire stockée (IC1), à appliquer une deuxième fonction logique prédéterminée à ces deux variables d'entrée et à délivrer une deuxième valeur de sortie correspondante, définissant ladite valeur initiale compteur ou ladite valeur finale compteur.

11. Dispositif selon l'une des revendications 7 à 9, caractérisé par

le fait que les moyens de traitement-système comportent des moyens de génération pseudo-aléatoire-système (22) aptes à générer ledit mot binaire pseudo-aléatoire, ce mot binaire pseudo-aléatoire accompagnant ladite information de demande de paiement (IDP).

12. Dispositif selon la revendication 11 prise en combinaison avec la revendication 8, caractérisé par le fait que les moyens de traitement-système comportent des premiers moyens de cryptage auxiliaires (20a) aptes à effectuer ledit premier cryptage auxiliaire de ladite première information spécifique (NS) pour recalculer la valeur de la première donnée auxiliaire (IC1), par le fait que les moyens de cryptage-système comportent des moyens analogues à ceux des moyens de cryptage-boîtier

et par le fait que les moyens de cryptage-système sont aptes à déterminer la deuxième valeur de gain cryptée (VF2) à partir de la valeur de la première donnée auxiliaire recalculée (IC1) et du mot binaire pseudo-aléatoire (MBA).

13. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les moyens de mémoire sont aptes à stocker une deuxième donnée auxiliaire prédéterminée (IC3), et par le fait qu'en présence de la demande de paiement émanant du joueur, les moyens de traitement-système sont aptes à effectuer un traitement de vérification (81) de la valeur de cette deuxième donnée auxiliaire, avant de délivrer ladite information de demande de paiement au boîtier.

14. Dispositif selon la revendication 13, caractérisé par le fait que les moyens de traitement-système comportent des deuxièmes moyens de cryptage auxiliaires (20b) aptes à effectuer un deuxième cryptage auxiliaire d'une deuxième information spécifique au système de contrôle, pour déterminer la deuxième donnée auxiliaire (IC3) au plus tard à la réception de ladite information d'autorisation de jeu, par le boîtier,

par le fait que les moyens de traitement-système sont aptes à stocker ladite deuxième information spécifique et la deuxième donnée auxiliaire (IC3) dans les moyens de mémoire (M2),

par le fait que les deuxièmes moyens de cryptage auxiliaires sont

aptes à lire la deuxième information spécifique et la deuxième donnée auxiliaire dans les moyens de mémoire du boîtier, et à comparer la valeur de la deuxième donnée auxiliaire lue avec celle recalculée par les deuxièmes moyens de cryptage auxiliaires à partir de la deuxième information spécifique lue.

15. Dispositif selon l'une des revendications précédentes caractérisé par le fait que les moyens de mémoire sont aptes à stocker, avant la réception de ladite information d'autorisation de jeu, une donnée d'authentification du boîtier (IC2),

et par le fait que la réception de ladite information d'autorisation de jeu est conditionnée à la vérification de cette donnée d'authentification.

16. Dispositif selon la revendication 15, caractérisé par le fait que la donnée d'authentification résulte d'un cryptage d'authentification d'une troisième information spécifique au boîtier (NS),

par le fait que les moyens de traitement-système comportent des moyens de cryptage d'authentification (21) aptes à recalculer la donnée d'authentification (IC2) à partir de la troisième information spécifique pour vérifier la valeur de cette troisième information spécifique lue dans les moyens de mémoire (M2).

17. Dispositif selon l'une des revendications 8 à 16, caractérisé par le fait que le premier et deuxième cryptage auxiliaire ainsi que le cryptage d'authentification comportent des algorithmes de cryptage à clé, et par le fait que la deuxième donnée auxiliaire et la donnée d'authentification sont des certificats cryptés des deuxième et troisième informations spécifiques.

18. Dispositif selon l'une des revendications 8 à 17, caractérisé par le fait que les première et troisième informations spécifiques comportent un authentifiant spécifique au boîtier tel que le numéro de série du boîtier, et par le fait que les moyens de traitement-système comportent des moyens de lecture du numéro de série.

19. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les moyens de mémoire comportent deux mémoires (M1, M2), l'une d'entre elles contenant la première donnée auxiliaire, l'autre contenant d'abord la donnée d'authentification (IC2)

puis, après vérification de cette dernière, la deuxième donnée auxiliaire (IC3).

20. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les moyens de mémoire comportent un compteur d'état (48) apte à contenir une information d'état représentative du résultat du jeu, ainsi qu'un compteur de paiement (49) apte à contenir une information de paiement représentative d'un paiement déjà effectué ou non encore effectué au joueur,

par le fait, qu'en présence de la demande de paiement émanant du joueur, les moyens de traitement-système sont aptes à lire en outre les contenus des compteurs d'état et de paiement avant de délivrer ladite information de demande de paiement au boîtier.

21. Dispositif selon l'une des revendications précédentes, caractérisé par le fait qu'il comporte des moyens d'alimentation (35, 36) autorisant le fonctionnement de certains au moins des moyens du boîtier avant la réception de l'information d'autorisation de jeu.

22. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que le boîtier est inapte au jeu à la suite d'une comparaison entre une donnée de référence et une donnée de jeu représentative d'un jeu perdant et/ou après un paiement effectif au joueur.

23. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que l'interface de communication comporte des moyens (28) de restitution au joueur d'une information de résultat représentative du résultat de la comparaison entre les données de jeu et de référence, lui indiquant s'il a perdu ou gagné.

24. Dispositif selon l'une des revendication précédente, caractérisé par le fait que les moyens de mémoire sont aptes à stocker une pluralité de données de référence, et

par le fait qu'une pluralité de données de jeu sont susceptibles d'être introduites par le joueur.

25. Dispositif selon la revendication 24, caractérisé par le fait que les données de jeu sont introduites successivement, chaque donnée de jeu introduite étant comparée à une donnée de référence prédéterminée,

et par le fait qu'une donnée de jeu ne peut être introduite par l'interface de communication qu'en cas d'une concordance entre la donnée de jeu précédemment introduite et la donnée de référence correspondante,

et par le fait qu'à chaque concordance correspond une information de gain différente (NG1,... NG10).

26. Dispositif selon les revendications 23 et 25, caractérisé par le fait que l'information de résultat comporte l'affichage d'une information de niveau de gain correspondant à l'information de gain contenue dans les moyens de mémoire.

27. Dispositif selon l'une des revendications 24 à 26, caractérisé par le fait que les moyens de mémoire comportent un compteur de gain (50) apte à contenir successivement des mots binaires de gain prédéterminés représentatifs des informations de gain successives, chaque mot binaire différant du mot suivant et du mot précédent par au moins deux bits.

28. Dispositif selon l'une des revendications 24 à 27, prise en combinaison avec la revendication 20, caractérisé par le fait que le compteur d'état (48) est apte à contenir successivement des mots binaires d'état prédéterminés représentatifs des informations d'état successives, chaque mot binaire d'état différant du mot suivant et du mot précédent par au moins deux bits.

29. Dispositif selon l'une des revendications précédentes prise en combinaison avec les revendications 4 et 24, caractérisé par le fait que les premiers moyens de génération aléatoire comportent une pluralité de compteurs de jeu (53-1,... 53-10), chaque compteur étant susceptible de contenir une donnée de référence et est associé à une introduction de donnée de jeu par le joueur.

30. Dispositif selon la revendication 29, caractérisé par le fait que la réception de ladite information d'autorisation de jeu (DV) stoppe le fonctionnement des compteurs, la pluralité de données de référence étant alors la pluralité de valeurs qu'avaient les compteurs à la réception de cette information d'autorisation de jeu.

31. Dispositif selon l'une des revendications 1 à 28 prise en combinaison avec les revendications 4 et 25, caractérisé par le fait que

le compteur est associé à toutes les introductions successives des données de jeu par le joueur, et par le fait que l'introduction d'une donnée de jeu par le joueur fige le compteur correspondant à une valeur définissant la valeur de référence associée à cette donnée de jeu.

32. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que le système de contrôle comporte une interface de dialogue (14, 15) apte à recevoir ladite demande de paiement émanant du joueur.

33. Dispositif selon la revendication 32, caractérisé par le fait qu'en présence d'une demande de vérification d'information de gain émanant du joueur, les moyens de traitement-système sont aptes à lire les contenus des compteurs de gain, d'état, et de paiement et à communiquer les résultats de cette lecture sur l'interface de dialogue.

34. Dispositif selon l'une des revendications précédentes, caractérisé par le fait qu'en présence d'une demande de paiement émanant du joueur, les moyens de traitement-système sont aptes à transmettre à l'interface-système d'entrée/sortie une demande de statut (ST1) en réponse à laquelle les moyens de traitement-boîtier délivrent ladite information de gain à l'interface-boîtier d'entrée/sortie.

35. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que le système de contrôle comporte au moins une station, telle qu'un terminal.

36. Dispositif selon les revendications 14 et 35, caractérisé par le fait que la deuxième information spécifique comporte le numéro de série de la station, la date de la vente du boîtier au joueur et le numéro d'ordre de cette vente à cette date.

37. Dispositif selon la revendication 35 ou 36, caractérisé par le fait que le système de contrôle comporte une pluralité de stations de structure analogue, les informations d'autorisation de jeu et de demande de paiement pouvant être délivrées par la même station ou par deux stations différentes.

38. Dispositif selon l'une des revendications 35 à 37, caractérisé par le fait que chaque boîtier possède un authentifiant unique, par le fait que le système de contrôle comporte des moyens de stockage (23)

d'une liste d'authentifiants des boîtiers gagnants et payés,
par le fait qu'en présence d'une demande de paiement émanant du joueur et correspondant à un gain supérieur à une valeur de gain prédéterminée, les moyens de traitement-système sont aptes à vérifier si l'authentifiant du boîtier concerné se situe déjà dans ladite liste.

39. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que le boîtier comporte un circuit intégré câblé (37) incorporant les moyens de traitement-boîtier et les moyens de mémoire du boîtier.

40. Boîtier appartenant au dispositif selon l'une des revendications 1 à 39.

41. Système de contrôle appartenant au dispositif selon l'une des revendications 1 à 39.

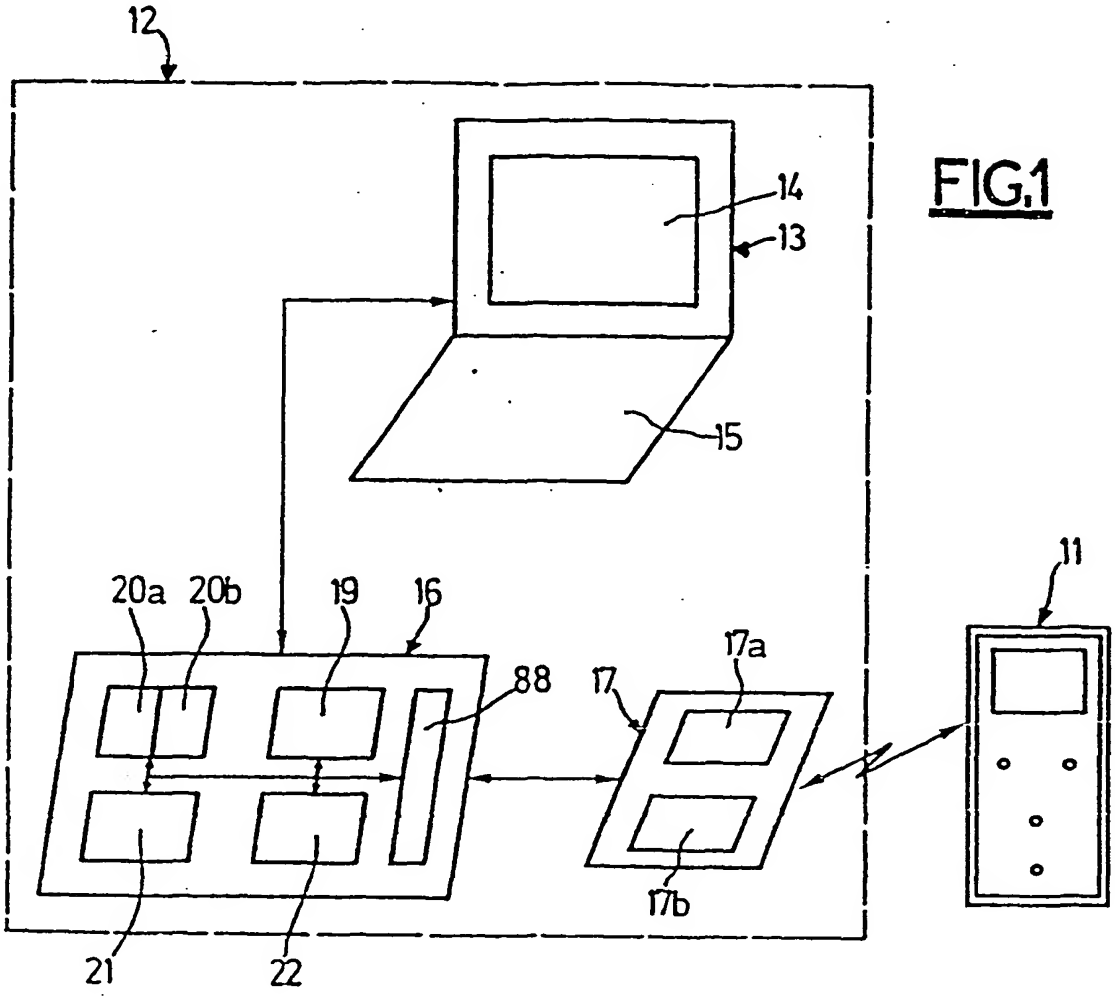


FIG.1

FIG.2

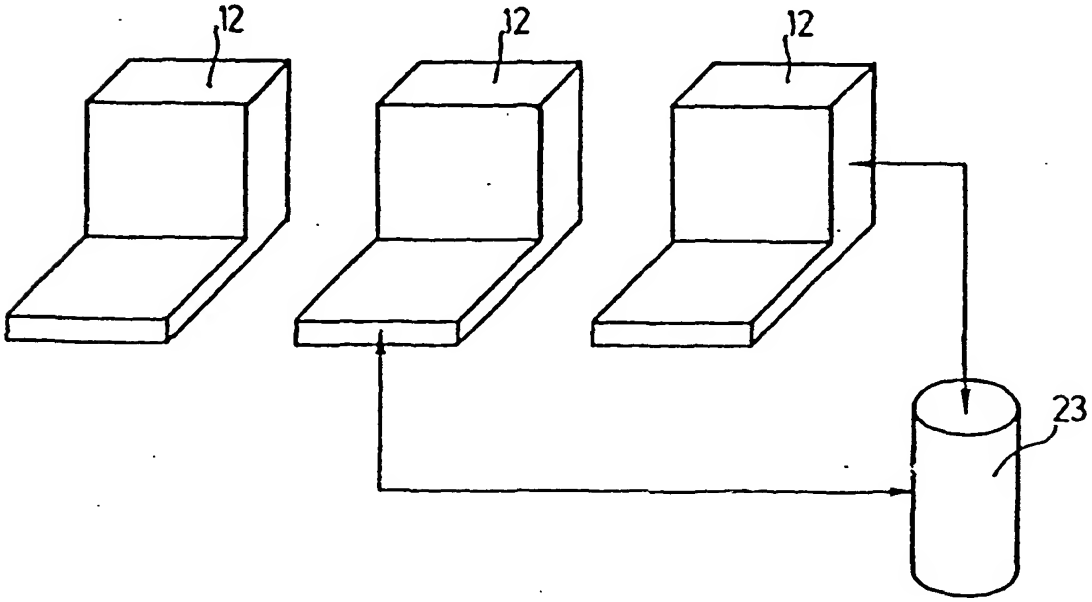


FIG.3a

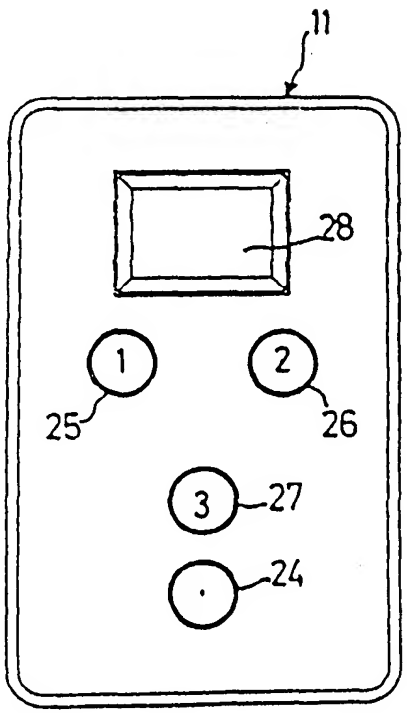


FIG.3b

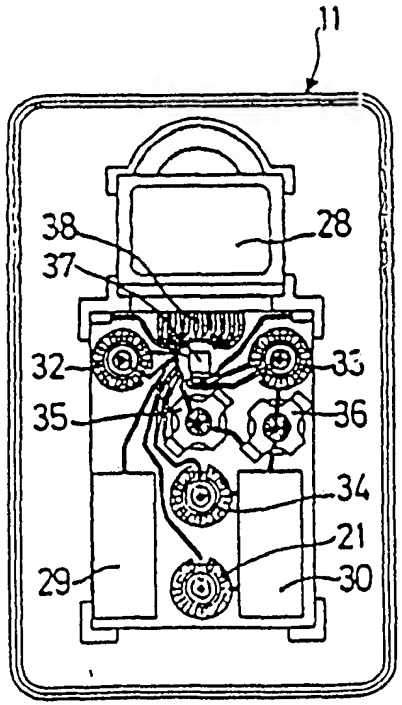
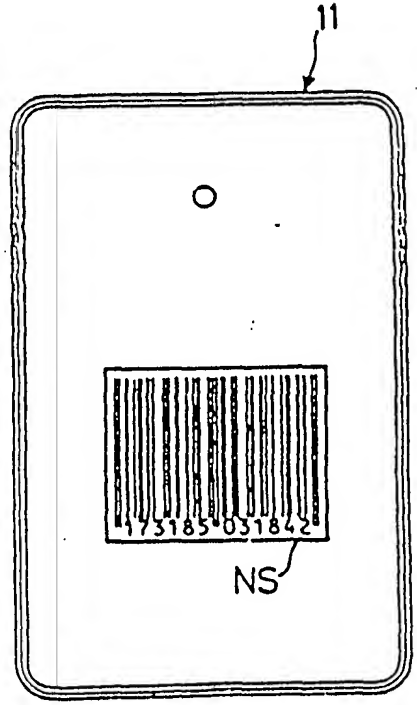


FIG.3c



2697653

FIG.4

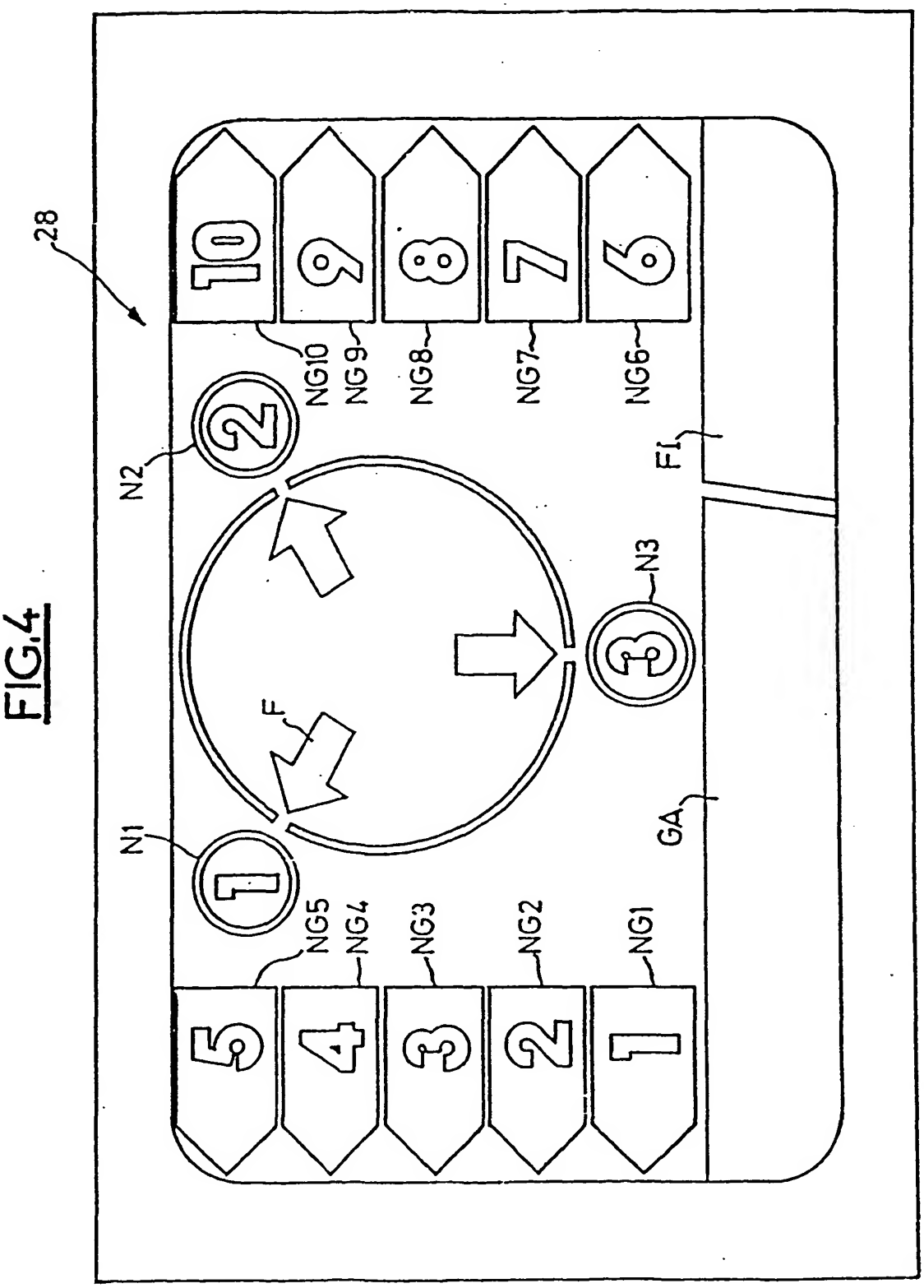

28
10
9
8
7
6
NG10
NG9
NG8
NG7
NG6
N2
2
FI
N3
3
F
N1
1
GA
5
4
3
2
1
NG5
NG4
NG3
NG2
NG1

FIG.5

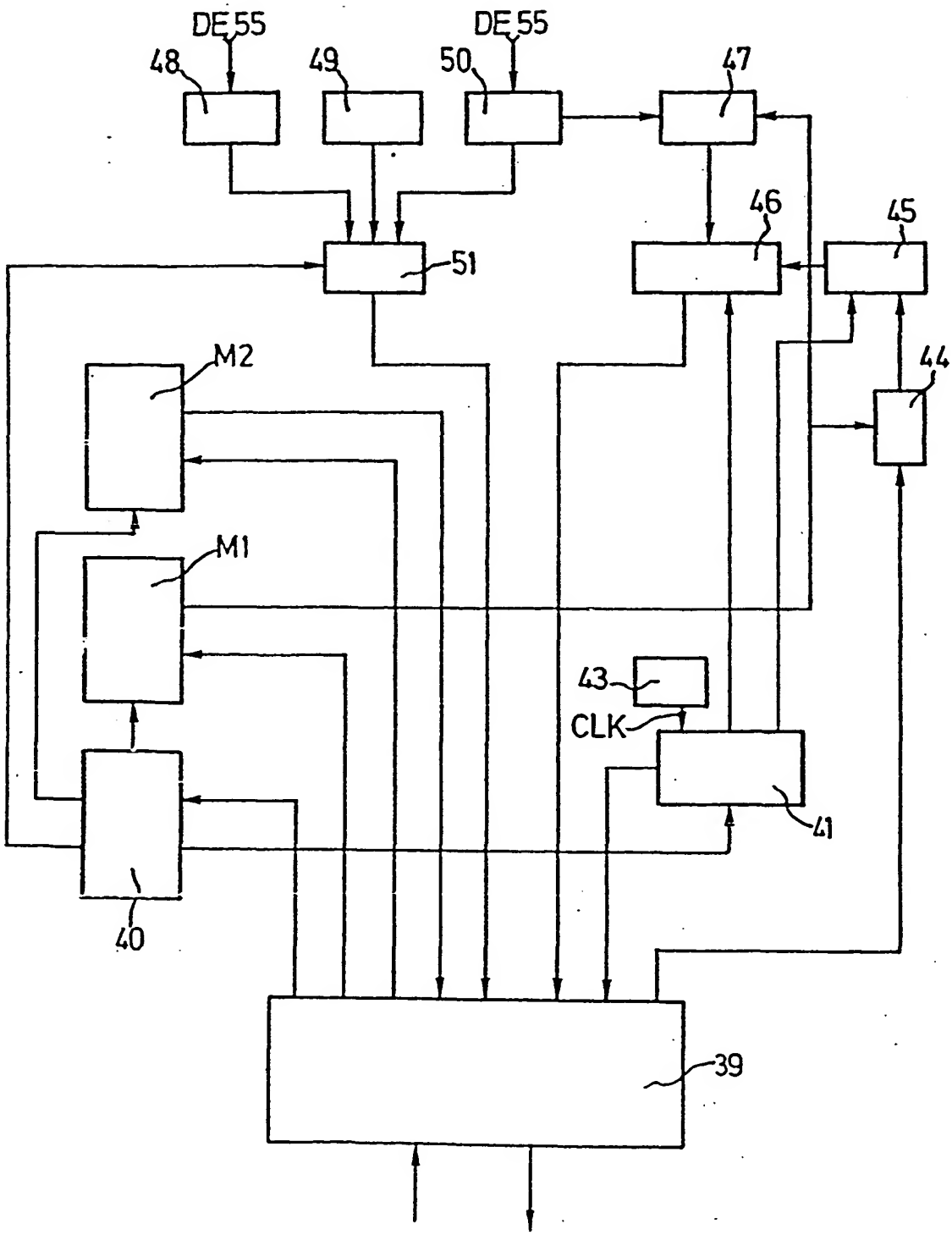


FIG.6

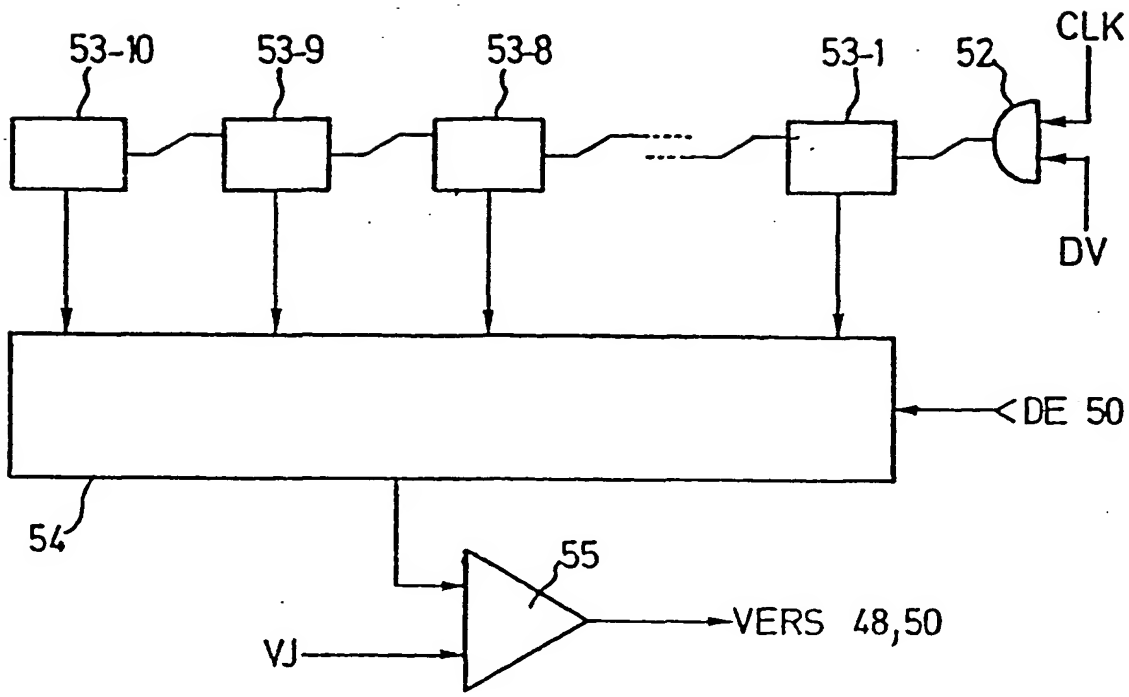

53-10
53-9
53-8
53-1
52
CLK
DV
DE 50
54
55
VJ
VERS 48,50

FIG.7

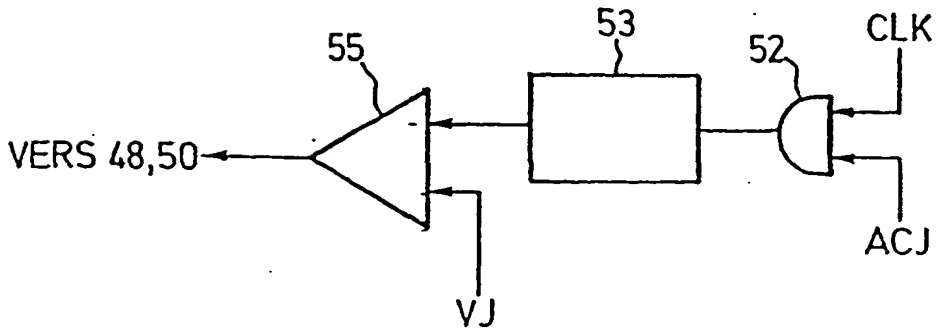

55
53
52
CLK
VERS 48,50
ACJ
VJ

FIG.8

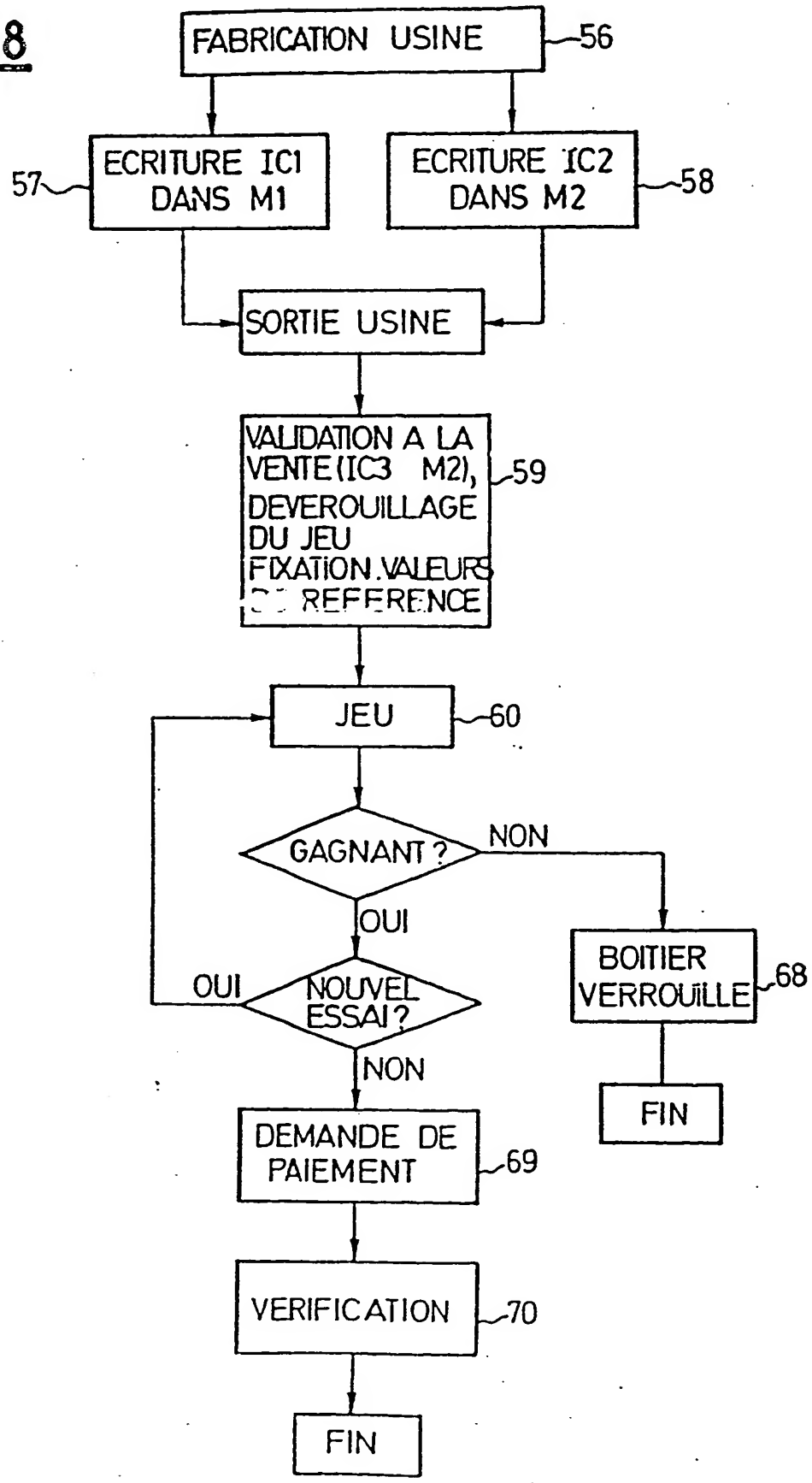
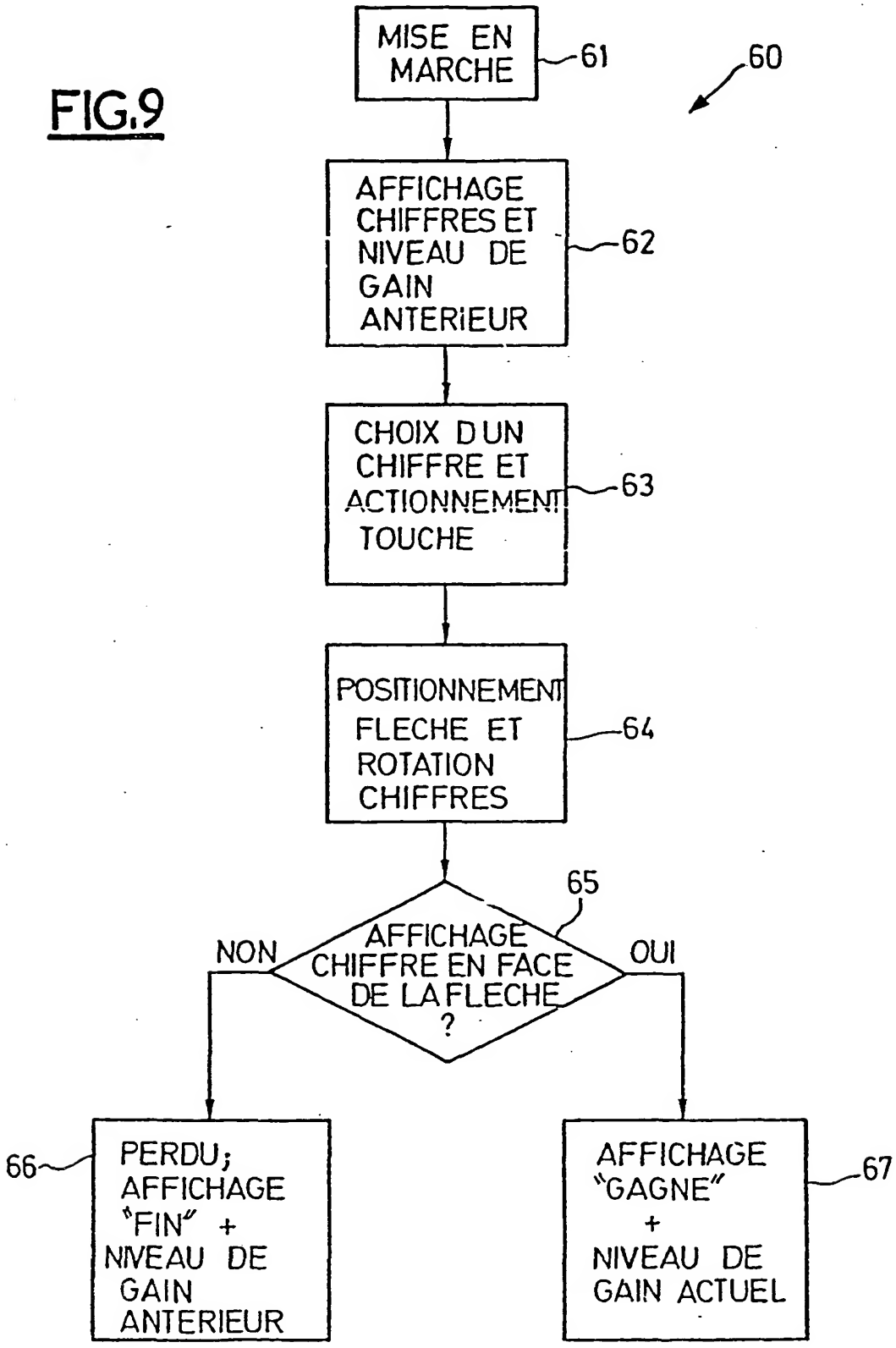

FABRICATION USINE
56
ECRITURE IC1 DANS M1
57
ECRITURE IC2 DANS M2
58
SORTIE USINE
VALIDATION A LA VENTE (IC3 M2), DEVEROUILLAGE DU JEU FIXATION VALEURS DE REFERENCE
59
JEU
60
GAGNANT ?
NON
OUI
BOITIER VERROUILLE
68
OUI
NOUVEL ESSAI ?
NON
FIN
DEMANDE DE PAIEMENT
69
VERIFICATION
70
FIN

FIG.9


MISE EN MARCHE
61
60
AFFICHAGE CHIFFRES ET NIVEAU DE GAIN ANTERIEUR
62
CHOIX D UN CHIFFRE ET ACTIONNEMENT TOUCHE
63
POSITIONNEMENT FLECHE ET ROTATION CHIFFRES
64
65
AFFICHAGE CHIFFRE EN FACE DE LA FLECHE ?
NON
OUI
66
PERDU; AFFICHAGE "FIN" + NIVEAU DE GAIN ANTERIEUR
AFFICHAGE "GAGNE" + NIVEAU DE GAIN ACTUEL
67

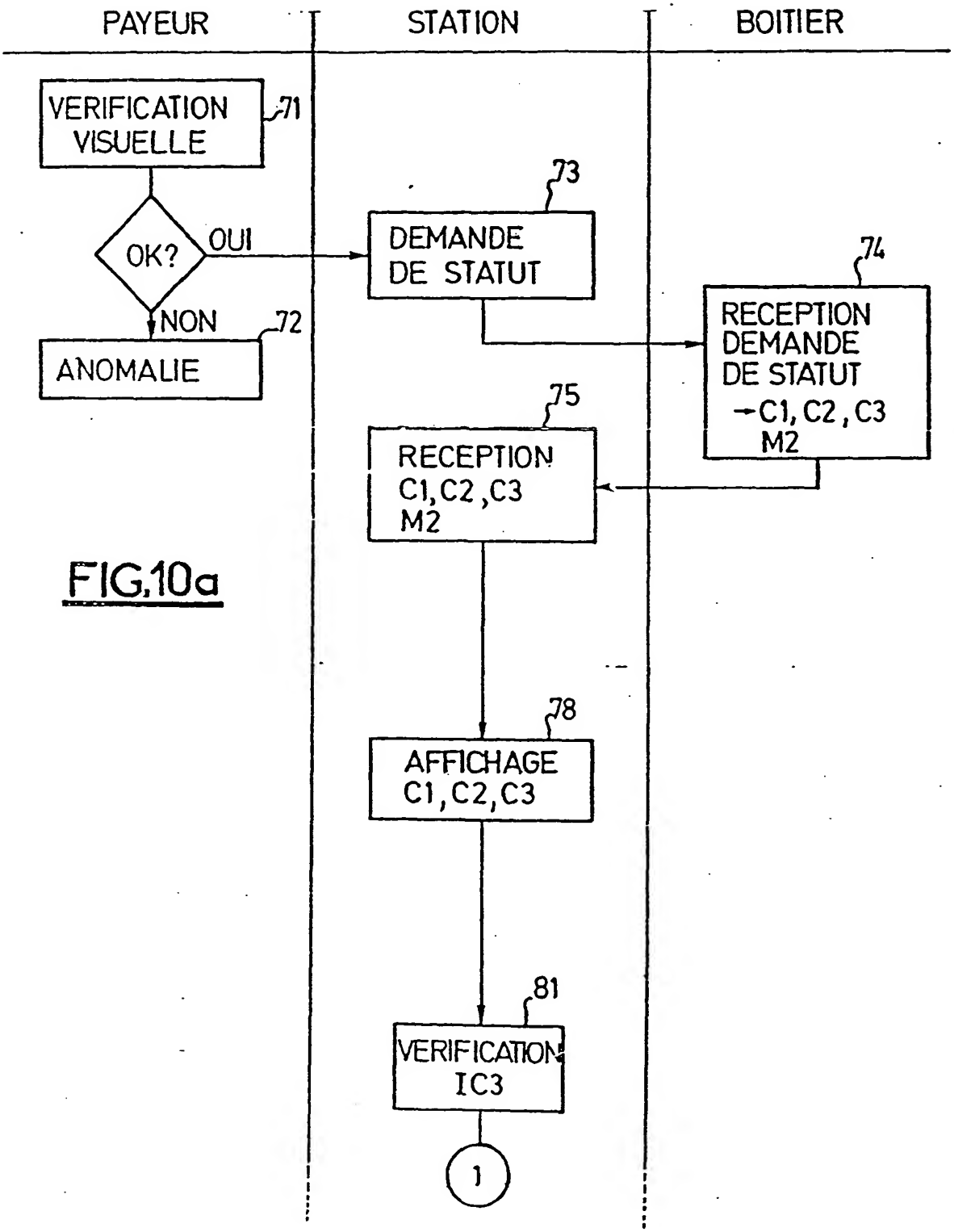

PAYEUR
STATION
BOITIER
VERIFICATION VISUELLE
71
OK?
OUI
NON
72
ANOMALIE
73
DEMANDE DE STATUT
74
RECEPTION DEMANDE DE STATUT
-C1, C2, C3
M2
75
RECEPTION
C1, C2, C3
M2
78
AFFICHAGE
C1, C2, C3
81
VERIFICATION
IC3
1

FIG.10a

FIG.10b

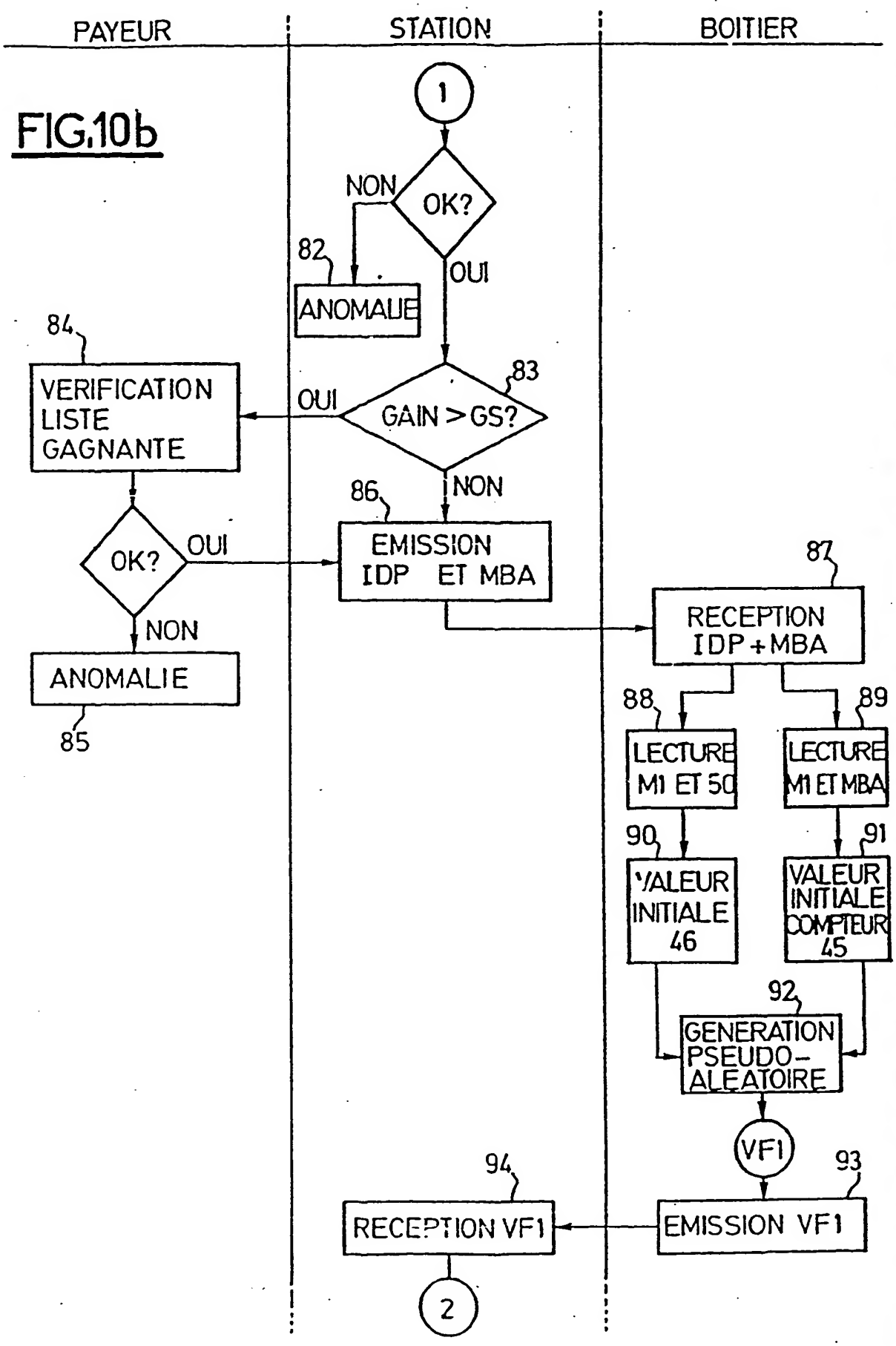
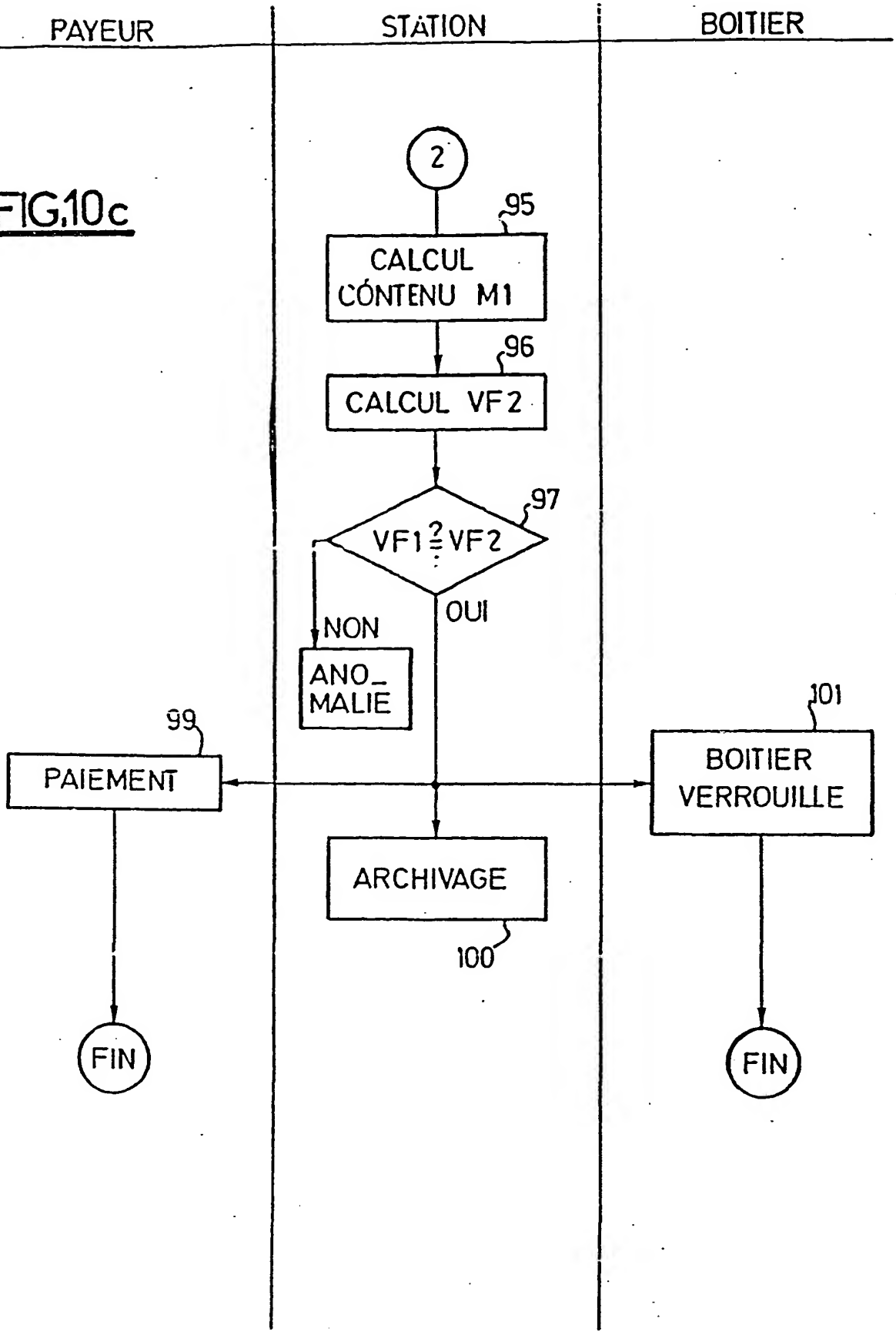

PAYEUR
STATION
BOITIER
1
NON
OK?
OUI
82
ANOMALIE
84
VERIFICATION LISTE GAGNANTE
OUI
83
GAIN > GS?
NON
86
EMISSION IDP ET MBA
OK?
OUI
NON
ANOMALIE
85
87
RECEPTION IDP + MBA
88
LECTURE M1 ET 50
89
LECTURE M1 ET MBA
90
VALEUR INITIALE 46
91
VALEUR INITIALE COMPTEUR 45
92
GENERATION PSEUDO-ALEATOIRE
VF1
93
EMISSION VF1
94
RECEPTION VF1
2

FIG.10c


PAYEUR
STATION
BOITIER
2
95
CALCUL CONTENU M1
96
CALCUL VF2
97
VF1 ? VF2
NON
OUI
ANO_MALIE
99
PAIEMENT
101
BOITIER VERROUILLE
ARCHIVAGE
100
FIN
FIN

REPUBLIQUE FRANÇAISE

2697653

N° d'enregistrement national

INSTITUT NATIONAL de la PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

FR 9213239
FA 478979

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	WO-A-8 902 139 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) * abrégé * * page 3, ligne 13 - page 5, ligne 12 *	1
A	WO-A-9 106 931 (RAHA) * abrégé *	1
A	EP-A-0 450 520 (GAMOT) * colonne 2, ligne 43 - colonne 3, ligne 2 * * colonne 4, ligne 54 - colonne 5, ligne 34 *	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G07F

Date d'achèvement de la recherche: 13 JUILLET 1993

Examinateur: TACCOEN J-F.P.L.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

4

EPO FORM 1503 03.82 (P0413)

TCA Translation

REPUBLIC OF FRANCE

Publication No.: 2,697,653
(Use only for reprint orders)

NATIONAL INSTITUTE OF
INDUSTRIAL PROPERTY
PARIS

National registration No.: 92 13239

Int. Cls.: G 07 C 15/00

APPLICATION FOR INVENTION PATENT A1

Application date: 11/4/92

Applicant(s): Corporation named INFO TELECOM - FR and mixed economy corporation called: LA FRANCAISE DES JEUX - FR.

Priority: /no entry/

Inventor(s): Reibel, Jean-Michel, Simon, Pierre-Luc, Bigonneau, Eric, and Bouedec, Jean-Etienne.

Date of publication of the application: 5/6/94 Bulletin 94/18.

List of documents cited in the preliminary research report: See the end of this brochure.

References to other related national documents: /no entry/

Principal(s): /no entry/

Mandatary: Bureau D.A. Casalonga - Josse.

Electronic system implementing a game of chance.

A portable unit (11) has memory circuits that can store at least one set of reference data, and comparison media that can compare said reference data to game data introduced by the player through a communication interface, whereby one of these two data sets is a randomly generated value. Gain information depending at least on the result of said comparison is stored in the memory, and unit encryption media, in response to predetermined payment request information (PRI) received, can establish a first encrypted gain value based on said gain information. An external station (12) outside the unit (11) contains an input/output interface (17), which communicates with the interface of the unit, and processors (16) which, in the presence of a request for payment by the player, can read said gain information contained in the memory of the unit. System encryption media (19), analog to the unit encryption media, establish a second encrypted gain value based on said gain information being read. Pay-off to the player depends on the matching of the two encrypted gain values.
/In margin:/ FF 2,697,653 - A1 /Drawing/

TCA Translation

Electronic system implementing a game of chance.

The present invention relates to an electronic system implementing a game of chance.

Currently, there are various known games of chance allowing a player to win money after paying a starting wager. Thus, for example, in the "loto" /lottery/ game (registered trademark), the player marks a series of numbers on a ticket which must be validated with a specialized agency, paying a price corresponding to the starting wager. Subsequently, a supervised drawing of lots takes place at a chosen venue, and the players holding a winning ticket may withdraw their gain from a payor entity.

Compared to these classic games, which require the use of paper and drawings of lots on predetermined dates, valid for all players, the invention provides a radically different concept of a system implementing a game of chance.

It is an object of the invention to provide an autonomous, portable unit allowing a player to make one or several wagers, the success or failure of which determine a score, or gain level, according to predetermined game rules. Said unit also constitutes the transaction element for the payment of the winnings, and comprises all the elements necessary for the verification of such winnings. In addition to this portable, stand-alone unit, there is a control system, outside the unit, which allows the payor entity to make necessary verifications before paying off the winnings.

Another object of the invention is to provide, inside the electronic unit itself, the drawing of the reference data to which the game data chosen by the player are compared. A further object of the invention is to allow simulation of one or several castings of dice, performing, inside the unit itself, a drawing of the game data, which are then compared to the predetermined reference data.

A very important consideration, inherent to such a gaming device, is the fight against fraud. In this regard, another object of the invention is to provide several securing and verification

levels, referring both to the origin of the portable unit and to the content of its information concerning, on the one hand, the "lose" or "win" aspects of the game, and, on the other hand, the value of the gain accumulated by the player, which may be quite significant.

Therefore, the invention provides an electronic system for implementing a game of chance, comprising:

a) a portable unit, comprising

- an input/output unit interface that can receive predetermined information authorizing the game, without which the unit cannot be used to play,
- a communication interface with the player,
- memory circuits capable of storing at least one set of reference data,
- unit processor, comprising:
- comparison media, which compare said reference data to the game data introduced by the player through the communication interface, whereby one of these two sets of data is a randomly generated value,
- media which can establish gain information, depending at least on the result of said comparison, and store this gain information in the memory, and
- unit encryption media, which, in response to a predetermined payment request received by the input/output unit interface, establish a first encrypted gain value based on said gain information, and deliver such first encrypted value to the unit interface, and

b) a control system, external to the unit, comprising

- an input/output system interface, which communicates with the input/output unit interface, and
- system processors, which,

. in the presence of a payment request from the player, read said gain information contained in the memory of the unit, and deliver said payment request information to the input/output system interface, and which include

. system encryption media, analog to the unit encryption media, which establish a second encrypted gain value based on said gain information being read, as well as comparison media that compare the two encrypted gain values; the actual payment of the winnings to the player is then subject at least to the matching of the two encrypted gain values.

Professionals know that the term "random" associated here to the generation of reference data or game data, is generally a mathematical concept, and that, in a practical embodiment of "random" generation, such generation is pseudo or quasi random, even though it is practically impossible to predict the data being generated. However, the term "random" is used here to reflect the practical impossibility, for a third party, to predict the game data or the reference data.

In one embodiment, system processors can transmit said predetermined game authorization information. On the other hand, in order to read gain information, in the presence of a payment request from the player, system processors can transmit a status request to the input/output system interface, in response to which unit processors deliver said gain information to the input/output unit interface.

In one embodiment, unit processors have a first set of random generators that can randomly generate said reference data from a predetermined series of values, while the communication interface has data entry media, allowing the player to choose his game data from the same predetermined series of values.

In order to assure the random drawing of the reference data, the first set of random generators conveniently include a game counter that operates from the start, prior to receiving said predetermined game authorization information; such counter can be stopped when a selected stop information is received, and can memorize the value it showed when stopped; this stop value determines said reference data.

The stop information preferably consists of said game authorization information.

In a variation, it is possible to design a game in which reference data are, for example, constants established in the rules of the game, the game data being randomly chosen by the player, in the way dice are cast. In such a variation, unit processors may include a secondary set of random generators, controlled by the action of the player, which can randomly deliver said game data, whereby the reference data are predetermined data stored in the memory.

To enhance security in the verification of the game information, the memory can store a first predetermined ancillary set of data, and the unit encryption media can generate the first encrypted gain value based on said gain information and said first set of ancillary data.

The first set of ancillary data is conveniently obtained based on a first ancillary encryption of at least a first set of information specific to the unit, such as its serial number, and is present in the memory before the receipt of the game authorization information.

In one embodiment, unit encryption media include:

- a pseudo-random gain encryption generator, which can be initialized at an initial value, and operate until it receives a stop command, in which case the first gain value is the value delivered by the pseudo-random gain encryption generator, upon receiving said stop command,

- a first logical circuit which can receive, as input variables, said gain information and at least part of the first ancillary data stored, apply a first logical predetermined function to these two input variables, and deliver a first corresponding output value, defining said initial value of the pseudo-random gain encryption generator, and

- an ancillary counter, which can count up or down, from an initial counter value to a final counter value; said command to stop the operation of the pseudo-random gain encryption generator is then delivered by the ancillary counter, when said final counter value is reached.

Unit encryption media also preferably include a second logical circuit that can receive as input variables a pseudo-random binary word, and at least a second part of the first ancillary data stored, apply a second logical predetermined function to these two input variables, and deliver a second corresponding output value, defining said initial counter value or said final counter value.

The system processors conveniently include system pseudo-random encryption media that can generate said pseudo-random binary word, which pseudo-random binary word accompanies said payment request information.

To verify the first encrypted gain value, system processors have a first set of ancillary encryption media which can perform said first ancillary encryption of said first specific information, in order to recalculate the value of the first ancillary data; on the other hand, system encryption media are analog to the unit encryption media, and can determine the second encrypted gain value based on the value of the first ancillary value recalculated, and on the pseudo-random binary word. This second encrypted gain value will then be compared to the first.

To verify again before payment, the memory conveniently can store a second predetermined ancillary value, and, in the presence of the player's payment request, system processors can verify the value of this second ancillary value, before delivering said payment request information to the unit. This second ancillary value can be a certificate, through an encryption algorithm with secret or public code, consisting of an identification specific to the control system, such as the serial number of a sale terminal.

To verify the origin of the unit, a convenient feature makes the memory capable of storing an identification of the unit, before receiving said game authorization information; the receipt of said game authorization information is then subject to the verification of this identification.

This identification data can result from an authentication encryption of a third item of information specific to the unit; this can be a certification of the serial number of the unit,

obtained from an encryption algorithm with secret or public code, using a key other than that reserved for the second ancillary data.

In this case, the system processors preferably contain authentication encryption media that can recalculate the identification data based on the third specific information, in order to verify the value of this third specific information read in the memory.

The serial number of the unit can be found in the memory of the unit. It can also be read by an appropriate reading device, such as an optical scanner, if the serial number appears in the form of a bar code on a label apposed on the unit.

In one embodiment, the memory has two levels, one containing the first ancillary data, the other containing first the identification data and then, after verifying the latter, the second ancillary data.

On the other hand, the memory can include a status counter that can contain status information representing the result of the game, as well as a payment counter that can contain payment information on a payment already made, or not yet made to the player.

In the presence of a payment request from the player, system processors can read, in addition, the content of the payment status counters, before delivering said payment request information to the unit.

The unit conveniently contains a power source, allowing the operation of at least some of these media, such as game counters and memory circuits, before receiving game authorization information.

The unit conveniently cannot play after a comparison between reference data and game data indicating a losing game and/or after an actual payment is made to the player.

The communication interface preferably includes media to give the player result information concerning the result of the comparison between game data and reference data, indicating whether he lost or won.

In one embodiment of the invention, the memory can store several reference data, and several game data which can be entered by the player.

These game data can be entered successively, each game datum entered being compared to a predetermined reference datum; a game datum cannot be entered by the communication interface unless the game data previously entered and the corresponding reference data match, whereby different gain information corresponds to each match.

Result information then conveniently displays the gain level corresponding to the gain information contained in the memory.

Memory circuits are preferably equipped with a gain counter that can successively contain predetermined binary gain words representing successive gain information, each binary word being different than the next and the preceding word by at least two bits. This allows having binary words sufficiently different between them, to properly differentiate the corresponding gain information, and especially to avoid errors caused, for example, by a mistaken reading or writing of a single bit. Equally, the status counter can conveniently contain successively predetermined status binary words representing successive status information, each binary word being different than the next and the preceding word by at least two bits.

When several game data must be entered by the player, especially successively, the first random generator preferably includes several game counters, each of which can contain reference data associated to game data entered by the player. Then, the receipt of said game authorization information may be set to stop the operation of all counters; then the multiple reference data are the multiple values found in the counters when receiving such game authorization information. In other words, the reference data is drawn once and for all, before the player enters the game data. However, it can be set so that a drawing takes place for each game datum entered. In this case, a single counter can be associated to all successive entries of game data by the player; when the player

enters game data, the counter is frozen at a value defining the reference value associated to such game data.

The control system conveniently includes a dialogue interface with the player, which can receive a payment request. This dialogue interface can be used for other purposes as well. Thus, in the presence of a request for verification of gain information from the player, the system processors can read the content of the gain counters, status counters, and payment counters, and communicate the results of this reading on the dialogue interface.

The control system can include at least one station, such as a terminal, and preferably several stations with analog structure, whereby game authorization and payment request information is delivered by the same station, or by two different stations.

To make another verification, especially when the gain is significant, the control system conveniently includes storage of a list of identification data of the winning and paid units and, in the presence of a payment request from the player, for a gain exceeding the predetermined gain value, system processors can verify whether the identification of the unit concerned is already found in said list.

Another object of the invention is a unit and a control system pertaining to such electronic device for a game of chance.

Other advantages and characteristics of the invention will appear from the examination of the detailed description of an embodiment, not limited thereto, and illustrated in drawings, as follows:

- figure 1 represents schematically a station and a unit according to the invention,
- figure 2 illustrates a network of stations,
- figures 3a, 3b, 3c represent in more detail the unit in figure 1,
- figure 4 represents a display screen of the unit,
- figures 5, 6 and 7 represent schematic synopses of the wired architecture of an ASIC component incorporated into the unit, and
- figures 8, 9, 10a, 10b, 10c represent operating layouts of

the device, and how the game is activated.

As illustrated in figure 1, the electronic gaming device has a portable unit 11 and a control system 12, external to the unit 12, and including an input/output system interface 17, including here two copper fields 17a and 17b that can communicate with the analog copper fields of an input/output interface of the unit 11, in order to exchange data by capacitive coupling.

In addition to this input/output interface 17, the control system 12 includes system processors 16, connected to this interface 17, as well as to a dialogue interface 13, with a user such as the seller or payor agent. This dialogue interface has a display screen 14, as well as a keyboard 15, for example for entering commands.

The system processors 16 are incorporated into an electronic card built around a micro-controller communicating with the interface 17 through an input/output register 88. As can be seen more in detail below, when the device is in operation, the system processors 16 have system encryption media 19, first and second ancillary encryption media 20 and 20b, authentication encryption media 21, as well as a system pseudo-random generator 22, that can generate a pseudo-random binary word whose meaning will be explained below. In reality, these various media are implemented logically in the micro-controller of the system processors.

In figure 1, the system processors 16, the input/output system interface 17, and the dialogue interface 13, are materially grouped in a station, such as a terminal. For this purpose, one can use a classic microcomputer, such as, for example, an IBM PC. In this case, the dialogue interface 13 will have the screen and the keyboard of the microcomputer. Then, one can use an additional electronic card, that can be introduced into the microcomputer, incorporating the system processors, as well as an extension constituting the interface 17.

Although, in general, the control system can be incorporated into a single station, it is planned to use a station network 12 (figure 2), all with analog structure. At least some of these

stations can be linked to storage units 23 that can store, as we will see more in detail below, a list of identifications of units having obtained a winning game, and having caused an actual payment to the player.

The unit 11 is sized, above all, so that it can be hand-held. On its front, (figure 3a), it has a key 24 which turns it on to activate at least some of its components, such as, for example, the display screen 28. On the other hand, this example of embodiment contains three game keys 25, 26 and 27, bearing three figures (1, 2 and 3), representing three game data among which the player can choose.

On the back, (figure 3c), there is a label on which there appears, for instance, in bar code, the serial number NS of the unit. Here, this serial number constitutes a unique identification, specific to the unit.

Figure 3b schematically illustrates an internal view of the unit 11. It shows the electronic prints 21, 32, 33 and 34 of the keys 24, 25, 26 and 27. Two copper fields 29 and 30, which are part of an input/output unit interface, can communicate with the two matching copper fields 17a and 17b of a station 12. Autonomous power sources 35 and 36, such as batteries, assure the autonomy of the portable unit and, as we will see below, permanently supply power to certain components of the unit.

While the three game keys 25, 26, 27, and the display screen 28 form a communication interface with the player, an essential element of the invention is here a specific integrated wired circuit (ASIC: Application Specific Integrated Circuit) bearing reference 37, and, as we will see in more detail below, comprising the unit processors, as well as the memory circuits. This ASIC is linked by a connection network 38 to the game keys, power sources, as well as the display screen 28. Of course, instead of an ASIC component, a micro-controller could have been used, incorporating in the software at least some of the functions of the unit described below. However, the use of an ASIC reduces manufacturing costs, and makes the device under the invention more secure against

fraud. Indeed, it is more difficult for a defrauder to access and understand the architecture of a wiring diagram specifically built for an application, and incorporated into an ASIC, than to obtain the instructions of a software incorporated in the memory of a micro-controller program.

Figure 4 shows a display screen 28, such as it may appear to the player in the specific application of the game described in this example. At the bottom of the display screen there are two spaces GA and FI, where the messages "GAGNE" /win/ and "FIN" /end/ may appear, depending on whether the player won or lost in his game of chance. On the two sides of the screen there respectively appear two columns with spaces numbered 1, 2, 3, 4, 5 and 6, 7, 8, 9, 10. These spaces bear references NG1-NG10, and correspond to successive gain levels reached by the player during the game. In the middle of the display screen there are spaces for three arrows F, respectively positioned across from circular spaces N1, N2 and N3, inside which there appear the three figures 1, 2 and 3. As we will see below, one of these arrows F will mark the choice of the player after having pressed one of the game keys 25 to 27, while one of the spaces N1, N2 or N3 will mark the reference data randomly drawn by the unit itself.

Figure 5 shows schematically part of the elements contained in the component 37. First, there is an input/output serial/ parallel register 39, which is part of the input/output unit interface, and linked to the two copper fields 29a and 30. This register 39 is connected to a decoding circuit 40 which can decode the various items of information received by the register 39 (input/output, writing, reading). This decoding circuit 40 is linked to a formatting circuit 51, connected first to a status counter 48, such as a non-linear counter, which can contain status information representing the "loss" or "gain" result of the game, secondly to a counter 49, which can contain information on a payment actually made to the player, and thirdly, to a so-called gain counter 50, such as a non-linear counter, which can contain gain information depending on the result of the game. In response to a status

request, the formatting circuit can deliver to the input/output register 39 the contents C1, C2, C3 of the three aforementioned counters 48, 49 and 50.

The output of the gain counter 50 is also linked to the input of the first logical circuit 47, whose other input is linked to a first live memory M1. The output of the first logical circuit is linked to a pseudo-random generator called gain encryption generator 46, such as a polynomial counter or a cyclic generator, also controlled by an ancillary counter 45 which receives at its input the output of the second logical circuit 44, the two inputs of which are respectively linked to the memory M1 and to the input/output register 39. The output of the gain encryption generator 46 is linked to the register 39.

Also included are logical control media 41 for all these elements, sequenced by a clock signal CLK with a frequency, for example, of 500 kHz, delivered by an oscillator 43.

Another live memory M2, linked to the input/output register 39, is part, along with M1, of the memory of the unit.

Figures 6 and 7 illustrate in more detail the first random generation media capable of generating the reference data which will be compared to the data entered by the player.

Figure 6 represents an embodiment applicable to drawing of lots, made once for several successive reference data (ten, for example), corresponding respectively to potential successive game data entries made by the player.

A logical part ET 52 receives at the input the clock signal CLK, as well as game authorization information DV, the meaning of which will be explained in more detail later. The output of this logical port 52 is linked to the first module counter 2 (53-1) of a range of ten counters 53-1 to 53-10, connected in cascade, whose output is respectively linked to the ten inputs of a multiplexer 54, whose output is linked to the first input of a comparator 55. Each comparator can therefore display a content corresponding to one of the three figures 1, 2 and 3. This multiplexer 54 is controlled, concerning the choice of its input path, by the output

of the gain counter 50. The other input of the comparator 55 receives the value VJ /"valeur de jeu" = game value/ of the game data entered by the player. The output of this comparator is linked to the status counter 58 and to the gain counter 50.

As we will see below, figure 7 illustrates a more particularly adapted embodiment, either for successive drawings associated respectively to the successive entries of game data made by the player, or to the random generation of game data which will be analogous, for example, to the casting of dice by the player. In this latter case, the reference data which will be compared to the randomly generated game data may be a constant stored in the memory of the unit. In this embodiment, the logical port 52 receives, instead of the game authorization information DV, the signal ACI of game data entered by the player on the communication interface. In this case, there is only one counter 53, linked to this logical port 52, the output of which is linked to the first input of the comparator 55.

Now we are going to describe more in detail the operation of the device under the invention, referring more particularly to figures 8 to 10c.

During manufacture at the factory (stage 56), a first set of ancillary data IC1 is stored in the memory M1, while a set of authentication data IC2 is stored in the memory M2 (stage 57 and stage 58). The first set of ancillary data IC1 constitutes a first securization, which will be used for actual payment of winnings to the player. In general, it results from a first ancillary encryption of information specific to the unit. More precisely, this is, for example, encrypted information obtained from a serial number NS of the unit through an encryption algorithm of the secret code type, such as that known by the abbreviation DES (Data Encryption Standard), and using a first secret code for this purpose. It would also be possible to use an encryption algorithm with public code, such as that known by the abbreviation RSA (Rivest Shamir Adelman).

The set of identification data IC2 also consists of

authentication encryption of information specific to the unit. Concretely, this is an encryption of the serial number of the unit, based on a secret (or possibly public) code algorithm, with a different code than that used for the information IC1. This data set IC2 is, in fact, a certificate of the serial number NS.

In order to preserve the content of the live memories M1 and M2, the unit will be permanently fed by its power sources installed at the factory. Therefore, said counters 53-1 to 53-10 operate from the manufacture stage of the unit at the factory.

However, at this stage, the unit is unable to play, or locked. In other words, the unit processors are inactive, and a player who obtains such unit would not be able to enter game data using the keys 25-27.

When released from the factory, the unit is stored in a sales facility equipped with a control station 12. When such a unit is sold to a player, it is first validated (stage 59). With the unit set on the unit interface 17, the unit processors 16 read the content of the memory M2, and the authentication encryption media 21 recalculate the authentication data IC2, based on the serial number NS and the value of the secret code used (also present in the memory of the station). For this purpose, the unit processors can know the serial number NS of the unit, either because it is directly stored in the memory M2 of the unit, or by optically reading, with a proper reader, the bar code located on the back of the unit. The matching of the authentication data with the data present in the memory M2 before this validation stage 59 allows making a first verification concerning the origin of the unit, and thus assuring that, a priori, the unit is authentic.

After completing this verification of origin, the second ancillary encryption media 20b of the unit processors determine a second set of ancillary encrypted data IC3, also based on information specific to the selling station, and a secret (or possibly public) code encryption algorithm, using a third code, different than the first two. Practically, the second ancillary encryption media use as unit-specific information its serial

number, the date of the sale, as well as a sequence number of the sale on that date, and determine the encrypted certificate of this unit-specific information. Then, the unit processors store this station-specific information, as well as the certificate IC3, in the memory M2.

The match between the authentication data set IC2, stored in the memory M2, and the recalculated data, also leads to the issuance of the game authorization information DV by the station processor; on the one hand, this will activate the unit processor in order to make the unit ready to play and, on the other hand, it will stop the operation of the game counters 53-1 to 53-10. This game authorization information, as well as the status request, are actually special commands issued by the station, at the receipt of which the unit processors perform predetermined operations. It is noteworthy that, in this embodiment, the set of reference data is then the set of values shown by the counters 53-1 to 53-10 when receiving the game authorization information. These reference data will be saved in the counters 53-1 to 53-10 for comparison with game data. The drawing of all reference data was therefore done once only. On the other hand, the quick pace of the operation of the counters, as well as the random character of the instant the counters are started at the factory, and the instant the information DV is received, contribute to the "random" character of the reference data generated.

Of course, in the variation illustrated in figure 7, with successive drawings of reference data, the receipt of the game authorization information DV has only the effect of activating the unit processors, and of unlocking the unit to make it ready to play.

The player now has a unit which is ready to play.

The game stage proper 60, here corresponding to a particular example of game, is illustrated in more detail in figure 9. When the unit is activated (stage 61) by pressing the key 24, the screen 28 displays (stage 62) the figures 1, 2 and 3 in the spaces N1, N2 and N3, as well as the previous gain level. If the player has never

before played with this unit, there is, of course, no display of the previous gain level.

In stage 63, the player chooses a figure and presses the corresponding key 25-27, thus entering his game data. The arrow F, pointing to the spaces N1, N2 or N3, according to the digit chosen by the player, is displayed, and unit processors activate a visual animation software, commonly called "chain" by professionals, which causes the figures 1, 2 and 3 to spin on the display screen 28, simulating the movement of a roulette in a roulette game. Then, the "chain" simulates the deceleration of the roulette, and the figure corresponding to the reference data contained in the first game counter 53-1 is displayed in the corresponding location on the display screen 28 (stages 64, 65).

If the figure is displayed facing the arrow F which marked the game data chosen by the player (stage 67), the player wins. In this case, the word "GAGNE" /wins/ is displayed in the GA location, and the gain level 1 is displayed in the NG1 location. Otherwise (stage 66), i.e. if the figure corresponding to the reference data is not displayed facing the arrow F, the player lost, and the word "FIN" /end/ is displayed in the FI location. In this case, the unit processor locks (stage 68) the communication interface with the player, in the sense that the latter can no longer enter game data with the keys 25-27. In other words, the unit is again made unable to play, and can be thrown out, for example.

If he wins, the player has two possibilities. He either decides to stop playing and request payment of his winnings, by going to the station 12, or he decides to try his chance once more, by choosing again a game data set which he enters by using the keys 24-27. Then the game repeats stages 63 to 66 or 67. In the embodiment illustrated in figure 6, the content of the gain counter allows selecting the input path of the multiplexer 54, since this gain counter contains different gain information for each winning attempt of the player. Thus, in this case, on the second attempt, the second counter 53-2 of the chain will be selected, and its content, corresponding to the second reference data set, will be

compared to the game data entered by the player. The player can thus try his chance ten times one after the other, hoping to reach the gain level 10. With each winning attempt, his current gain level is displayed, and is higher than the preceding gain level. On the contrary, if during this sequence of events, an attempt loses, the unit can no longer play, and the preceding gain level remains displayed. Of course, the player can make a further attempt only if he won on the previous attempt, i.e. if the reference data in his preceding attempt matched the game data he entered at that time.

In the embodiment illustrated in figure 7, the ten reference sets of data corresponding to the ten gain levels are not predetermined in advance. The counter 53 works until a key 24-27 is pressed by the player, marking his choice of game data. This action ACJ /activating game choice/ then blocks the counter 53 on a value defining the randomly generated reference value, associated to the game data entered by the player during his attempt. After displaying a possible winning result, the counter 52 continues to work, and will again freeze on another value, if the player enters another game value.

The variation in figure 7 is also compatible with another type of game, consisting, this time, of comparing the constant predetermined reference values stored in memory, to game data entered randomly by the player. This simulates a casting of dice by the player. In this case, the receipt of the signal in ACJ, caused by the player's pressing an appropriate key on the unit, causes the counter 53 to stop, marking the random generation of the game data, which will be then compared to the reference value (here also indicated by VJ) stored in memory.

If a player who won and reached a certain gain level decides to stop playing and to request payment of his winnings, he makes a payment request 69 to a station 12, which then begins an in-depth verification stage 70. We must note, at this point, that the player can request such payment from the same station that sold him his unit, or from a similar station.

We now refer more particularly to figures 10a to 10c, in order

to describe this verification stage.

This stage begins with a visual verification 71 by the agent in charge of making payments. This visual verification consists of verifying the display of the word "GAGNE," as well as the display of a gain level. If no error 72 appears, the unit is then placed on the input/output interface 17 of the station, and the system processors deliver a status request (stage 73) through the unit processors. Upon receipt 74 of this status request ST1, the unit processors deliver to the input/output register 39 the respective contents C1, C2, C3 of the counters 48, 49 and 50, as well as the content of the memory M2. The respective contents C1, C2, C3 are then displayed in "clear" on the screen 14 of the dialogue interface of the station (stage 78). This constitutes another visual verification which, however, is not sufficient proof for actual payment of the winnings to the player, as explained below.

A verification stage 81 then begins, consisting of verifying the value of the second ancillary data IC3 contained in the memory M2. For this purpose, the second ancillary encryption media of the station system processors read the station-specific information (serial number of the station, date of sale and sequence order) in the memory M2, and recalculate the certificate IC3 of this specific information, in order to compare it to that contained in the memory M2.

A non-matching of these two data sets IC3 also leads to an error 82 which can interrupt the payment process. Otherwise, the system processors compare the gain information from the gain counter 50 to a predetermined gain value GS. If the gain is higher than this value GS, the system processors verify whether the identification of the unit in question, i.e. its serial number, is not already on a list of winning unit identifications which were already paid. If this is the case, there would also be an error 85, which interrupts the payment process. If the station 12 is not linked to the storage media 23 of this list, the player is asked to go to a station linked to this list. Of course, the player can be asked to change stations immediately after the visual verification

71.

If the gain is lower than the GS value, or if the gain is higher than the GS value and the unit is not on the winning list, the system processors issue (stage 86) payment request information (IDP) accompanied by an aleatory binary word MBA. Upon receipt 87 of the information IDP and the binary word MBA through the unit input/output interface, the encryption media (44, 45, 46 and 47) of the unit can generate a first encrypted gain value VF1, based on the gain information contained in the gain counter 50 and the first ancillary data set IC1 contained in the memory M1 (stages 88-92).

For this purpose, the pseudo-random gain encryption generator 46 can be initialized at an initial value, and operate until it receives a stop command. The first encrypted gain value VF1 is then the value delivered by the pseudo-random gain encryption generator 46 when receiving such stop command.

The first logical circuit 47 receives, as input variable, the gain information contained in the gain counter 50, and part of the first ancillary data set IC1 contained in the memory M1. This first circuit 47 then applies a first predetermined logical function, for example based on an exclusive OU /or/, to these two input variables, and delivers a first corresponding output value, which defines the initial value of the pseudo-random gain encryption generator 46.

The ancillary counter 45 can count up or down from an initial counter value to a final counter value. The command to stop the operation of the pseudo-random gain encryption generator is then delivered by the ancillary counter 45, when said final counter value is received.

The second logical circuit 44 is used here to define the initial counter value, or the final counter value, depending on whether the counter counts up or down.

This second logical circuit receives, as input variable, the pseudo-random binary word MBA and a second part of the first stored ancillary data set IC1. A second predetermined logical function, preferably different than the first. is then applied to these two

input variables, and the second logical circuit 44 delivers a second output value, which defines the initial counter value or the final counter value.

Thus, the polynomial counter (for example) 46, is initialized at an initial value depending on the encrypted content of the memory M1 and on the gain information contained in the gain counter 50. This counter operates then until the ancillary counter 45 stops, the number of repetitions of the latter being defined pseudo-randomly with the help of the binary word MBA. When the counter 46 stops, its content, which defines the first encrypted gain value VF1, is delivered to the system processors of the station through the intermediary input/output register 39 (stages 93, 94).

The actual payment of the winnings to the player will take place only if this first encrypted gain value VF1, delivered by the unit, is identical to a second encrypted gain value VF2, established by the system encryption media 19 of the station. For this purpose, the first ancillary encryption media 20a of the station recalculate the first ancillary encrypted data IC1 based on the serial number of the unit and the corresponding secret code. This serial number can be stored in the memory M1, or read optically by an optical scanner. Starting from there, the system encryption media, which are similar to the unit encryption media (i.e. logical circuits and counters analogous to logical circuits 44, 47 and counters 45 and 46), calculate the second encrypted gain value, similarly to that used for the calculation of the first encrypted gain value, based on the information IC1 recalculated by the first ancillary encryption media, and the pseudo-random binary word MBA, which is known to the station because it is generated by the pseudo-random generation media of the system 22.

If the two sets of data do not match, a new error appears and interrupts the payment process. On the contrary, if they match, the payment 99 of the winnings is made to the player, the unit is locked (stage 101), the counter 49 is loaded with information concerning the payment made to the player, and the serial number of

this winning unit is stored (stage 100), either at the station itself, or in the storage media 23, especially in the event of a gain higher than the value GS.

The fact that the actual payment of the winnings to the player is subject to the matching of the two encrypted gain values VF1 and VF2 guarantees the payor entity against fraud, especially that caused by counterfeit units containing microprocessors programmed to simulate fake gain information values.

Although the other verification stages (status request. verification of data IC2 and IC3) are not indispensable, they conveniently contribute to increase securization against fraud. On the other hand, the professional would have understood that only the content of the counters 48, 49 and 50 have value of proof for the payor entity, and that the display of their content on the screen 14 or 28 is merely a visual indication. Thus, and also in order to increase securization, the gain counter 50 is conveniently designed to contain successively predetermined binary gain words representing successive gain information that the player could obtain if he successively won at each attempt. Each binary word is then different than the preceding and following words found on the list, by at least two bits. Such a precaution complicates further the task of a defrauder who would seek to modify the content of the gain counter, because he would have to modify two bits at a time, rather than one.

The same precaution can be conveniently used for the status counter 48, with a second predetermined list of binary words differing from each other by at least two bits. In addition, this brings double securization for the verification of the gain level obtained and the losing or winning status of the game at each attempt.

Finally, a player may wish to purchase a unit from a third party in order to continue the game. In this case, it is especially beneficial that the buyer can verify, in particular, the content of the gain counter. Thus, in the presence of a verification request concerning gain information coming from the buyer player, the

TCA Translation

system processors can read the contents of the gain, status and payment counters, and communicate the results of such reading on the screen 14 of the dialogue interface. Of course, in this case, the payment request information IDP is not delivered to the unit.

CLAIMS

1. Electronic device implementing a game of chance, comprising

a) a portable unit (11) containing

- an input/output unit interface (39, 29, 30) that can receive predetermined game authorization information without which the unit cannot play,

- a communication interface (24, 25, 26, 27, 28) with the player,

- memory circuits (M1, M2, 53-1,... 53-10, 48, 49, 50) that can store at least one reference data set,

- unit processor, containing

. comparison media (55) that can compare said reference data with game data entered by the player using the communication interface, one of these two data sets being a randomly generated value,

. media (50) that can establish gain information depending at least on the result of said comparison, and store such gain information in the memory (50), and

. unit encryption media (44-47) that, in response to predetermined payment request information (IDP) received by the input/output unit interface, can establish a first encrypted gain value (VF1) based on said game information, and deliver this first encrypted gain value to the unit interface, and

b) a control system (12), external to the unit (11), comprising

- an input/output system interface (17) that can communicate with the input/output unit interface, and

- system processors (16), that can,

. in the presence of a payment request from the player, read said gain information contained in the unit memory, and deliver said payment request information (IDP) to the input/output system interface, and comprise

. system encryption media (19), similar to the unit encryption media, which can establish a second encrypted gain value (VF2)

based on said gain information read, as well as comparison media that can compare the two encrypted gain values,

whereby the actual payment of the winnings to the player is subject at least to the matching of the two encrypted gain values.

2. Device according to claim 1, characterized by the fact that the system processors can transmit said predetermined game authorization information (DV).

3. Device according to claim 1 or 2, characterized by the fact that the unit processors include first random generation media (53-1,... 53-10) that can randomly generate said reference data from a predetermined series of values, while the communication interface has data entering media (25-27), allowing the player to choose his game data among the same predetermined series of values.

4. Device according to claim 3, characterized by the fact that the first random generation media have at least one game counter (53-1... 53-10) that operates from an initial instant preceding the receipt of said predetermined game authorization information (DV), this counter being liable to the stopped when receiving a chosen stop command (DV) and to save the value it shows when its operation stops, whereby said stop value defines said reference value.

5. Device according to claim 4, characterized by the fact that the stop information constitutes said game authorization information (DV).

6. Device according to claim 1 or 2, characterized by the fact that the unit processors include second random generation media (53), controlled by the action of the player, that can randomly deliver said game data, whereby the set of reference data is a set of data previously stored in the memory.

7. Device according to one of the preceding claims, characterized by the fact that the memory circuits (M1) can store a first set of predetermined ancillary data (IC1),
and by the fact that unit encryption media (44-47) can generate the first encrypted gain value (VF1) based on said gain information and said first set of ancillary data (IC1).

8. Device according to claim 7, characterized by the fact that

the first set of ancillary data is obtained based on a first ancillary encryption of at least a first item of information (NS) specific for the unit, and is present in memory (M1) before the receipt of the game authorization information (DV).

9. Device according to claim 7 or 8, characterized by the fact that the unit encryption media include:

- a pseudo-random gain encryption generator (46) that can be initialized at an initial value, and operate until it receives a stop command, in which case the first encrypted gain value (VF1) is the value delivered by the pseudo-random gain encryption generator, when receiving said stop command,
  - a first logical circuit (47) which can receive, as input variables, said gain information and at least part of the first ancillary data stored (IC1), apply a first logical predetermined function to these two input variables, and deliver a first corresponding output value, defining said initial value of the pseudo-random gain encryption generator, and
  - an ancillary counter (45), which can count up or down, from an initial counter value to a final counter value; said command to stop the operation of the pseudo-random gain encryption generator (46) is then delivered by the ancillary counter, when reaching said final counter value.

10. Device according to claim 9, characterized by the fact that the unit encryption media include a second logical circuit (44), which can receive, as input variable, the pseudo-random binary word (MBA) and at least a second part of the first stored set of ancillary data (IC1), apply a second predetermined logical function to these two input variables, and deliver a second corresponding output value, which defines said initial counter value or the final counter value.

11. Device according to one of the claims 7 to 9, characterized by the fact that the system processors have a system pseudo-random generator (22), that can generate a pseudo-random

binary word which accompanies said payment request information (IDP).

12. Device according to claim 11, combined with claim 8, characterized by the fact that system processors include the first ancillary encryption media (20a), which can perform the first ancillary encryption of the first specific information (NS) in order to recalculate the value of the first ancillary data (IC1), by the fact that system encryption media are similar to the unit encryption media
and by the fact that the system encryption media can determine the second encrypted gain value (VF2) based on the value of the first recalculated ancillary data (IC1) and the pseudo-random binary word (MBA).

13. Device according to one of the preceding claims, characterized by the fact that memory circuits can store a second set of predetermined ancillary data (IC3), and that, in the presence of a request for payment by the player, the system-encryption media can process a verification (81) of the value of this second set of ancillary data before delivering said payment request information to the unit.

14. Device according to claim 13, characterized by the fact that the system processors have a second set of ancillary encryption media (20b), which can perform a second ancillary encryption of a second information specific for the control system, in order to determine the second set of ancillary data (IC3), at the latest when receiving said game authorization information from the unit,
by the fact that the system processors can store said second specific information and the second set of ancillary data (IC3) in the memory (M2),
by the fact that the second ancillary encryption media can read the second specific information and the second set of ancillary data in the memory of the unit, and compare the value of the second set of ancillary data read to that recalculated by the second ancillary encryption media based on the second specific information read.

15. Device according to one of the preceding claims, characterized by the fact that the memory is able to store unit authentication data (IC2) before receiving said game authorization information,

and by the fact that the receipt of said game authorization information depends on the verification of these authentication data.

16. Device according to claim 15, characterized by the fact that the authentication data arise from the encryption of the authentication of a third information specific to the unit (NS),

by the fact that the system processors have authentication encryption media (21) that can recalculate the authentication data (IC2) based on the third specific information, in order to verify the value of this third specific information read in the memory (M2).

17. Device according to one of the claims 8 to 16, characterized by the fact that the first and second ancillary encryption, as well as the authentication encryption, have code encryption algorithms, and by the fact that the second ancillary data and the authentication data are encrypted certificates of the second and third specific information.

18. Device according to one of the claims 8 to 17, characterized by the fact that the first and third specific information have an identification specific to the unit, such as the serial number of the unit, and by the fact that the system processors have media that can read the serial number.

19. Device according to one of the preceding claims, characterized by the fact that the memory has two memory circuits (M1, M2), one of which contains the first ancillary data, and the other the first set of authentication data (IC2) and then, after verifying the latter, the second set of ancillary data (IC3).

20. Device according to one of the preceding claims, characterized by the fact that the memory has a status counter (48) which can contain status information representing the result of the game, as well as a payment counter (49), which can contain

information on a payment actually made to the player, or not yet made to the player,

by the fact that, in the presence of a payment request from the player, the system processors can also read the content of the status and payment counters, before delivering said payment request information to the unit.

21. Device according to one of the preceding claims, characterized by the fact that it has power supply media (35, 36), allowing at least certain unit features to function before receiving game authorization information.

22. Device according to one of the preceding claims, characterized by the fact that the unit cannot play after a comparison between reference data and game data showing a losing game and/or after an actual payment is made to the player.

23. Device according to one of the preceding claims, characterized by the fact that the communication interface has media (28) for returning to the player result information concerning the result of the comparison between game and reference data, indicating to him whether he lost or won.

24. Device according to one of the preceding claims, characterized by the fact that the memory circuits can store several reference data, and

by the fact that several game data can be entered by the player.

25. Device according to claim 24, characterized by the fact that game data are entered successively, each game datum entered being compared to a predetermined reference datum,

and by the fact that a game datum cannot be entered through the communication interface unless there is a match between the previously entered game datum and the corresponding reference datum,

and by the fact that to each match corresponds a different gain information item (NG1,... NG10).

26. Device according to claims 23 and 25, characterized by the fact that the result information comprises the display of gain

level information corresponding to the gain information contained in the memory.

27. Device according to one of the claims 24 to 26, characterized by the fact that the memory has a gain counter (50) that can successively contain predetermined binary gain words representing successive gain information, each binary word differing from the following and preceding word by at least two bits.

28. Device according to one of the claims 24 to 27, in combination with claim 20, characterized by the fact that the status counter (48) can contain successively predetermined status binary words representing successive gain information, each binary word differing from the following and preceding word by at least two bits.

29. Device according to one of the preceding claims, in combination with claims 4 and 24, characterized by the fact that the first random generation media have several game counters (53-1,... 53-10), each counter being capable of containing a reference datum, and being associated to the entering of a game datum by the player.

30. Device according to claim 29, characterized by the fact that the receipt of said game authorization information (DV) stops the operation of the counters, in which case the various reference data are the various values shown by the counters when they received this game authorization information.

31. Device according to one of the claims 1 to 28, in combination with claims 4 and 25, characterized by the fact that the counter is associated with every successive entering of game data by the player, and by the fact that the entering of a game datum by the player corresponds to a value defining the reference value associated to this game datum.

32. Device according to one of the preceding claims, characterized by the fact that the control system has a dialogue interface (14, 15) that can receive said payment request from the player.

33. Device according to claim 32, characterized by the fact that, in the presence of a request for verification of gain information from the player, the system processors can read the content of the gain counters, status counters, and payment counters, and communicate the results of this reading on the dialogue interface.

34. Device according to one of the preceding claims, characterized by the fact that, in the presence of a payment request from the player, the system processors can transmit to the input/output system interface a status request (STI), in response to which the unit processors deliver said gain information to the input/output unit interface.

35. Device according to one of the preceding claims, characterized by the fact that the control system has at least one station, such as a terminal.

36. Device according to claims 14 and 35, characterized by the fact that the second specific information has the serial number of the station, the date of sale of the unit to the player, and the sequence number of that sale on that date.

37. Device according to claim 35 or 36, characterized by the fact that the control system has several stations with analog structure, whereby game authorization information and payment request information can be delivered by the same station or by two different stations.

38. Device according to claims 35 to 37, characterized by the fact that each unit has a unique identification, by the fact that the control system has storage capacity (23) for a series of identifications of winning and paid units,
by the fact that, in the presence of a payment request from the player and corresponding to a gain higher than a predetermined gain value, system processors can verify whether the identification of the unit concerned is already on said list.

39. Device according to the preceding claims, characterized by the fact that the unit has a wired integrated circuit (37), containing the unit processors and the memory of the unit.

40. Unit pertaining to the device according to one of the claims 1 to 39.

41. Control system pertaining to the device according to one of the claims 1 to 39.

TCA Translation

Fig. 1

/Diagram/

Fig. 2

/Diagram/

Fig. 3c

/Diagram/

Fig. 3b

/Diagram/

Fig. 3a

/Diagram/

TCA Translation

Fig. 4

/Diagram/

TCA Translation

Fig. 5

/Diagram/

TCA Translation

Fig. 6

/Diagram/

"vers" = towards

Fig. 7

/Diagram/
"vers" = towards

Fig. 8

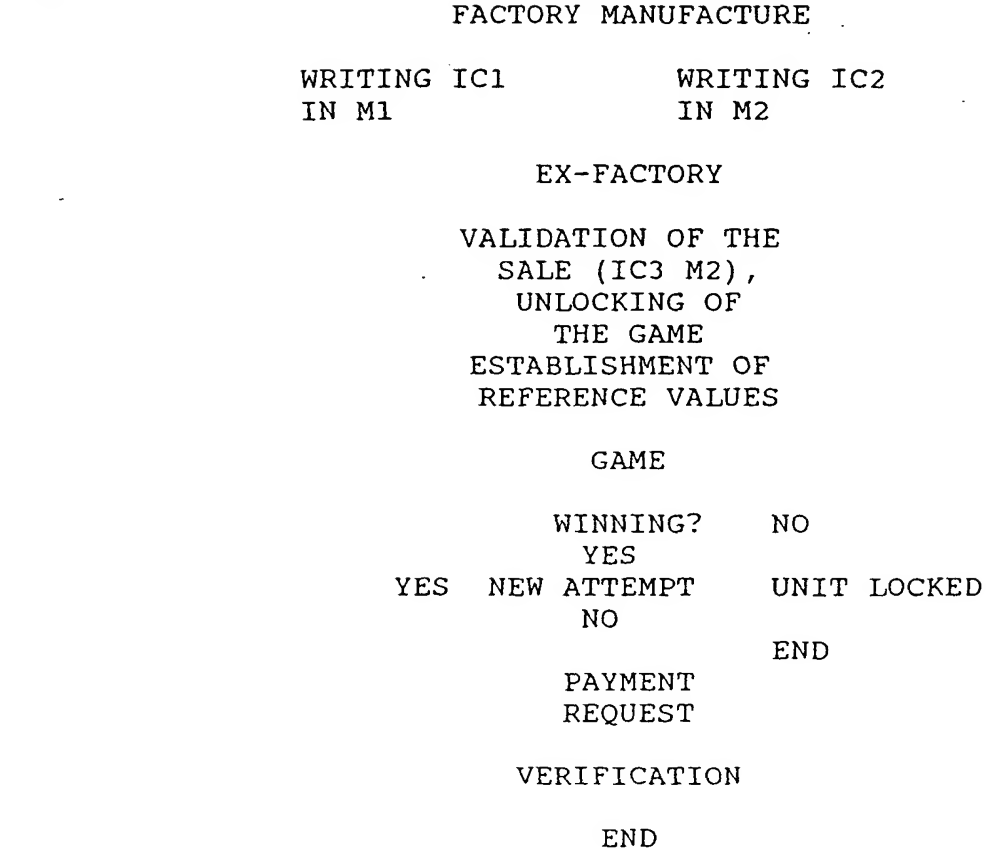

FACTORY MANUFACTURE
WRITING IC1 IN M1
WRITING IC2 IN M2
EX-FACTORY
VALIDATION OF THE SALE (IC3 M2), UNLOCKING OF THE GAME ESTABLISHMENT OF REFERENCE VALUES
GAME
WINNING?
YES
NO
YES
NEW ATTEMPT
NO
UNIT LOCKED
END
PAYMENT REQUEST
VERIFICATION
END

Fig. 9

TURNING ON

DISPLAY FIGURES AND PREVIOUS GAIN LEVEL

CHOICE OF FIGURE AND PRESSING OF A KEY

POSITIONING OF ARROW AND FIGURE ROTATION

NO — DISPLAY FIGURE ACROSS FROM THE ARROW ? — YES

LOSS; DISPLAY "END" + PREVIOUS GAIN LEVEL

DISPLAY "WIN" + CURRENT GAIN LEVEL

/see original for diagram/

Fig. 10a

PAYOR STATION UNIT

VISUAL
VERIFICATION

OK? YES STATUS REQUEST

RECEIPT STATUS
REQUEST
-> C1, C2, C3
M2

NO
ERROR

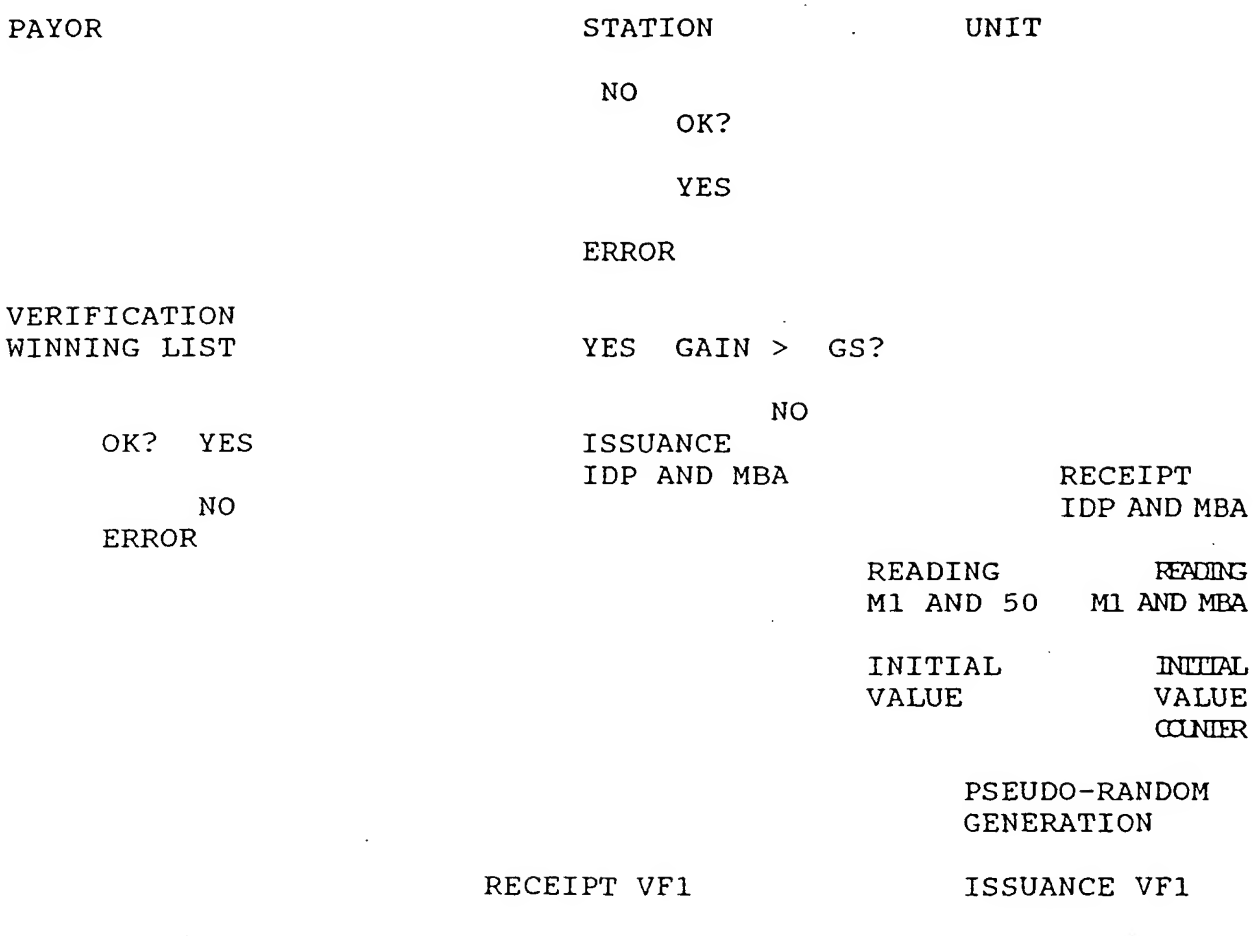
RECEIPT
C1, C2, C3
M2

DISPLAY
C1, C2, C3

VERIFICATION
IC3

/see original for diagram/

Fig. 10b



/see original for diagram/

Fig. 10c

PAYOR STATION UNIT

CALCULATION
CONTENT M1

CALCULATION VF2

VF1 =? VF2

NO YES
ERROR

PAYMENT

STORAGE UNIT LOCKED

END END

/see original for diagram/

TCA Translation

42 2697653

REPUBLIC OF FRANCE

NATIONAL INSTITUTE OF
INDUSTRIAL PROPERTY

National registration No.
FR 9213239
FA 478979

RESEARCH REPORT
issued based on the latest claims
registered before the beginning of the research

DOCUMENTS DEEMED PERTINENT		Claims concerned of the application examined
Category	Document quotation with indication of pertinent parts, if necessary	
A	WO-A-8 902 139 (AMERICAN TELEPHONE TELEGRAPH COMPANY) * summarized* * page 3, line 13 - page 5, line 12 *	1
A	WO-A-9 106 931 (RAHA) * summarized*	1
A	EP-A-O 450 520 (GANOT) *column 2, line 43 - column 3, line 2 * * column 4, line 54 - column 5, line 34*	

TECHNICAL FIELDS OF RESEARCH (Int'l Cl.5)
G07F

Date of research completion
JULY 13, 1993

/Illegible/
TACCOEN J-F.P.L.

CATEGORY OF DOCUMENTS CITED

X: Especially pertinent by itself
Y: Especially pertinent along with another document of the same category
A: Pertinent in opposition with one /illegible/ general technical claim

O: Non-written disclosure

P: Intercalary document

T: Theory in principle underlying the invention

E: Patent document dated prior to the application date, and which was not published other than on that application date or later

C: Cited in application

L: Cited for other reasons

/illegible/: Member of the same family, corresponding document